On the Immunity of Boolean Functions Against Fast Algebraic Attacks Using Bivariate Polynomial Representation

Meicheng Liu, Yin Zhang, and Dongdai Lin

SKLOIS, Institute of Information Engineering, CAS, Beijing 100195, P. R. China
meicheng.liu@gmail.com, zhangy@is.iscas.ac.cn, ddlin@iie.ac.cn

Abstract. In the last decade, algebraic and fast algebraic attacks are regarded as the most successful attacks on LFSR-based stream ciphers. Since the notion of algebraic immunity was introduced, the properties and constructions of Boolean functions with maximum algebraic immunity have been researched in a large number of papers. However, it is unclear whether these functions behave well against fast algebraic attacks. In this paper, we study the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation. Based on bivariate polynomial representation, we present a sufficient and necessary condition for a Boolean function to achieve good immunity against fast algebraic attacks, propose an efficient method for estimating the immunity of a large class of Boolean functions, including the functions of Q. Jin et al., and prove that the functions of D. Tang et al. achieve (almost) optimal immunity against fast algebraic attacks.

Keywords: Boolean functions, Algebraic immunity, Fast algebraic attacks

1 Introduction

Boolean functions are frequently used in the design of stream ciphers, block ciphers and hash functions. One of the most vital roles in cryptography of Boolean functions is to be used as filter and combination generators of stream ciphers based on linear feedback shift registers (LFSR). The study of the cryptographic criteria of Boolean functions is important because of the connections between known cryptanalytic attacks and these criteria.

In recent years, algebraic and fast algebraic attacks [1,6,7] have been regarded as the most successful attacks on LFSR-based stream ciphers. These attacks cleverly use over-defined systems of multi-variable nonlinear equations to recover the secret key. Algebraic attacks lower the degree of the equations by multiplying a nonzero function; fast algebraic attacks obtain equations of small degree by linear combination.

Thus the algebraic immunity ($\mathcal{AI}$), the minimum algebraic degree of annihilators of f or $f+1$, was introduced by W. Meier et al. [18] to measure the ability of Boolean functions to resist algebraic attacks. It was shown by N. Courtois and W. Meier [6] that maximum $\mathcal{AI}$ of n-variable Boolean functions is $\lceil \frac{n}{2} \rceil$. Constructions of Boolean functions with maximum $\mathcal{AI}$ were researched in a large number of papers, e.g., [9,14,15,4,22,23]. However, there are few results referring to constructions of Boolean functions with good immunity against fast algebraic attacks.

A preprocessing of fast algebraic attacks on LFSR-based stream ciphers, which use a Boolean function $f : GF(2)^n \to GF(2)$ as the filter or combination generator, is to find a function g of small degree such that the multiple gf has degree not too large. The resistance against fast algebraic attacks is not covered by algebraic immunity [8,2,16]. At Eurocrypt 2006, F. Armknecht et al. [2] introduced an effective algorithm for determining the immunity against fast algebraic attacks, and showed that a class of symmetric Boolean functions (the majority functions) have poor resistance against fast algebraic attacks despite their resistance against algebraic attacks. Later M. Liu et al. [16] stated that almost all the symmetric functions including these functions with good algebraic immunity behave badly against fast algebraic attacks. In [19] P. Rizomiliotis introduced three matrices to evaluate the behavior of Boolean functions against fast algebraic attacks using univariate polynomial representation while in [17] the authors used one matrix to evaluate the immunity for fast algebraic attacks.

In [7] N. Courtois proved that for any pair of positive integers (e, d) such that $e + d \geq n$, there is a nonzero function g of degree at most e such that gf has degree at most d. This result reveals an

upper bound on maximum immunity to fast algebraic attacks. It implies that the function f has maximum possible resistance against fast algebraic attacks, if for any pair of positive integers (e, d) such that $e+d < n$ and $e < n/2$, there is no nonzero function g of degree at most e such that gf has degree at most d. Such functions are said to be perfect algebraic immune ($\mathcal{PAI}$) [17]. Note that one can use the fast general attack by splitting the function into two $f = h + l$ with l being the linear part of f [7]. In this case, e equals 1 and d equals the degree of the function f, where g can be considered as the nonzero constant. Thus $\mathcal{PAI}$ functions have algebraic degree at least $n-1$. A $\mathcal{PAI}$ function also achieves maximum $\mathcal{AI}$. As a consequence, a $\mathcal{PAI}$ function has perfect immunity against classical and fast algebraic attacks. Besides, it is shown that a perfect algebraic immune function behaves good against probabilistic algebraic attacks as well [17]. Although preventing classical and fast algebraic attacks is not sufficient for resisting algebraic attacks on the augmented function [11], the resistance against these attacks depends on the update function and tap positions used in a stream cipher and in actual fact it is not a property of the Boolean function. In [17] the authors proved that there are n-variable $\mathcal{PAI}$ functions if and only if $n = 2^s$ or $2^s + 1$. More precisely, there exist n-variable $\mathcal{PAI}$ functions with degree $n-1$ (balanced functions) if and only if $n = 2^s + 1$; there exist n-variable $\mathcal{PAI}$ functions with degree n (unbalanced functions) if and only if $n = 2^s$.

Several classes of Boolean functions, e.g., [4,23,21], are observed through computer experiments by Armknecht's algorithm [2] to have good behavior against fast algebraic attacks, but in previous literature only Carlet-Feng functions are proven to be optimal against fast algebraic attacks as well as classical algebraic attacks [17].

In this paper, we study the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation. Based on this representation, we prove that a Boolean function $f(x, y)$ admits no nonzero function $g(x, y)$ of degree at most e such that the product $g(x, y)f(x, y)$ has degree at most d if and only if the matrix $B(f; e, d)$, whose elements are represented by the coefficients of the bivariate polynomial representation of the function f, has full column rank.

Further, we investigate the immunity against fast algebraic attacks for a large family of functions which has a form as

$$\tau(x, y) = \phi(xy^r) + (x^{2^k-1} + 1)\psi(y) + (y^{2^k-1} + 1)\varphi(x).$$

We first present several properties of the matrix $B(\tau; e, d)$. Two observations on this matrix are that after appropriate row transformations it can be represented by

$$\begin{pmatrix} * \\ B^*(\phi(xy^r); e, d) \end{pmatrix}, \tag{1}$$

and that after appropriate column transformations it can be represented by

$$\left(*,\ B_*(\phi(xy^r); e, d) \right), \tag{2}$$

where $B^*(\phi(xy^r); e, d)$ and $B_*(\phi(xy^r); e, d)$ are submatrices of $B(\phi(xy^r); e, d)$. Our observation on the matrix $B(\phi(xy^r); e, d)$ is that after appropriate matrix transformations it is a quasidiagonal matrix. Then, based on these properties, we propose an efficient method to determine the immunity of $\tau(x, y)$ against fast algebraic attacks through computations of submatrices of $B(\phi(xy^r); e, d)$.

Also we apply the technique to the family of functions which has a form as

$$\tau_{CF}(x, y) = \phi_{CF}(xy^r) + (x^{2^k-1} + 1)\psi(y) + (y^{2^k-1} + 1)\varphi(x),$$

where ϕ_{CF} is a Carlet-Feng function. Quite a number of functions are contained in this family, e.g., the functions of Z. Tu and Y. Deng [22], the functions of D. Tang et al. [21], and the functions of Q. Jin et al. [13]. Using the method treating Carlet-Feng functions in [17], we show that to ensure that the matrix $B^*(\phi(xy^r); e, d)$ has full column rank one only need to ensure the number of rows is greater than or equal to the number of columns of the submatrices. In particular, we prove that the family of the functions τ_{CF}

with $r = 1$, including the functions of D. Tang et al. [21], achieve (almost) optimal immunity against fast algebraic attacks.

The remainder of this paper is organized as follows. In Section 2 some basic concepts are provided. Section 3 generally studies the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation. Section 4 studies the immunity of the function $\tau(x, y)$ against fast algebraic attacks while Section 5 treats the function $\tau_{CF}(x, y)$. Section 6 concludes the paper.

2 Preliminary

Let $\mathbb{F}_2$ denote the binary field $GF(2)$ and $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Denote by $\mathbf{B}_n$ the set of all n-variable Boolean functions. An n-variable Boolean function f can be uniquely represented as its truth table, i.e., a binary string of length 2^n,

$$f = [f(0, 0, \cdots, 0), f(1, 0, \cdots, 0), \cdots, f(1, 1, \cdots, 1)].$$

The support of f is given by $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. The Hamming weight of f, denoted by $\mathrm{wt}(f)$, is the number of ones in the truth table of f. An n-variable function f is said to be balanced if its truth table contains equal number of zeros and ones, that is, $\mathrm{wt}(f) = 2^{n-1}$.

An n-variable Boolean function f can also be uniquely represented as a multivariate polynomial over $\mathbb{F}_2$,

$$f(x_1, \cdots, x_n) = \sum_{c \in \mathbb{F}_2^n} \lambda_c \prod_{i=1}^{n} x_i^{c_i},\ \lambda_c \in \mathbb{F}_2, c = (c_1, \cdots, c_n),$$

called the algebraic normal form (ANF). The algebraic degree of f, denoted by $\deg(f)$, is defined as $\max\{\mathrm{wt}(c) \mid a_c \neq 0\}$.

Let $\mathbb{F}_{2^n}$ denote the finite field $GF(2^n)$. The Boolean function f considered as a mapping from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ can be uniquely represented as

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,\ a_i \in \mathbb{F}_{2^n}, \tag{3}$$

where $f^2(x) \equiv f(x) (\mathrm{mod}\, x^{2^n} - x)$. Expression (3) is called the univariate polynomial representation of the function f. It is well known that $f^2(x) \equiv f(x) (\mathrm{mod}\, x^{2^n} - x)$ if and only if $a_0, a_{2^n-1} \in \mathbb{F}_2$ and for $1 \leq i \leq 2^n - 2$, $a_{2i \bmod (2^n-1)} = a_i^2$. The algebraic degree of the function f equals $\max\limits_{a_i \neq 0} \mathrm{wt}(i)$, where $i = \sum_{k=1}^{n} i_k 2^{k-1}$ is considered as $(i_1, i_2, \cdots, i_n) \in \mathbb{F}_2^n$.

Let α be a primitive element of $\mathbb{F}_{2^n}$. The a_i's of Expression (3) are given by $a_0 = f(0), a_{2^n-1} = f(0) + \sum_{j=0}^{2^n-2} f(\alpha^j)$ and

$$a_i = \sum_{j=0}^{2^n-2} f(\alpha^j) \alpha^{-ij},\ \text{for } 1 \leq i \leq 2^n - 2. \tag{4}$$

Let $n = n_1 + n_2$ $(n_1 \leq n_2)$ and denote by $\mathrm{lcm}(n_1, n_2)$ the least common multiple of positive integers n_1 and n_2. The Boolean function f considered as a mapping from $\mathbb{F}_{2^{n_1}} \times \mathbb{F}_{2^{n_2}}$ into $\mathbb{F}_2$ can be uniquely represented as

$$f(x, y) = \sum_{i=0}^{2^{n_1}-1} \sum_{j=0}^{2^{n_2}-1} a_{ij} x^i y^j,\ a_{ij} \in \mathbb{F}_{2^{\mathrm{lcm}(n_1,n_2)}}, \tag{5}$$

where $f^2(x, y) \equiv f(x, y) (\mathrm{mod}(x^{2^{n_1}} - x, y^{2^{n_2}} - y))$. Expression (5) is called the bivariate polynomial representation of the function f. We can see that $f^2(x, y) \equiv f(x, y) (\mathrm{mod}(x^{2^{n_1}} - x, y^{2^{n_2}} - y))$ if and only if $a_{2^{n_1}-1, 2^{n_2}-1} \in \mathbb{F}_2$ and for $0 \leq i \leq 2^{n_1} - 2$ and $0 \leq j \leq 2^{n_2} - 2$,

$$a_{2i,2j} = a_{ij}^2,$$

$$a_{2^{n_1}-1,2j} = a_{2^{n_1}-1,j}^2, \tag{6}$$
$$a_{2i,2^{n_2}-1} = a_{i,2^{n_2}-1}^2,$$

where $2i$ and $2j$ are considered as $2i \bmod (2^{n_1}-1)$ and $2j \bmod (2^{n_2}-1)$ respectively, which implies $a_{0,0}, a_{0,2^{n_2}-1}, a_{2^{n_1}-1,0} \in \mathbb{F}_2$. The algebraic degree of the function f equals $\max\limits_{a_{ij}\neq 0}\{\mathrm{wt}(i)+\mathrm{wt}(j)\}$.

An example of the bivariate polynomial representation is listed in Appendix A.

In particular, for $n = 2k$, the Boolean function f considered as a mapping from $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ into $\mathbb{F}_2$ can be uniquely represented as

$$f(x,y) = \sum_{i=0}^{2^k-1}\sum_{i=0}^{2^k-1} a_{ij}x^i y^j,\ a_{ij} \in \mathbb{F}_{2^k}, \tag{7}$$

where $f^2(x,y) \equiv f(x,y) (\mathrm{mod}(x^{2^k}-x, y^{2^k}-y))$.

For more details with regard to the representation of Boolean functions, we refer to [3].

The algebraic immunity of Boolean functions is defined as follows. Maximum algebraic immunity of n-variable Boolean functions is $\lceil \frac{n}{2} \rceil$ [6].

Definition 1 *[18] The algebraic immunity of a function $f \in \mathbf{B}_n$, denoted by $\mathcal{AI}(f)$, is defined as*

$$\mathcal{AI}(f) = \min\{\deg(g) \mid gf = 0 \text{ or } g(f+1) = 0, 0 \neq g \in \mathbf{B}_n\}.$$

If there is a nonzero Boolean function g with degree at most e such that the product gf has degree at most d, with e small and d not too large, then the Boolean function f is considered to be weak against fast algebraic attacks. The exact values of e and d for which a fast algebraic attack is feasible depends on several parameters, like the size of the memory and the key size of the stream cipher [12].

Theorem 1 *[17] Let $f \in \mathbf{B}_n$.*

If $\deg(f) < n$, then for $e < n/2$ such that $\binom{n-1}{e} \equiv 1 (\mathrm{mod}\, 2)$, there exists a nonzero function g with degree at most e such that the product gf has degree at most $n-e-1$. Further, if $n \neq 2^s+1$ and $\deg(f) < n$, then there exist an integer $e < n/2$ and a nonzero function g with degree at most e such that the product gf has degree at most $n-e-1$.

If $\deg(f) = n$, then for $e < n/2$ such that $\binom{n-1}{e} \equiv 0 (\mathrm{mod}\, 2)$, there exists a nonzero function g with degree at most e such that the product gf has degree at most $n-e-1$. Further, if $n \neq 2^s$ and $\deg(f) = n$, then there exist an integer $e < n/2$ and a nonzero function g with degree at most e such that the product gf has degree at most $n-e-1$.

3 The immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation

In this section we focus on the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation.

We define the operation "$\circ_k$" by $a \circ_k u = c \in \{0,1,\cdots,2^k-1\}$ for $a,u \in \{0,1,\cdots,2^k-1\}$ with c such that $x^{a \circ u} \bmod (x^{2^k}-x) = x^c$, where "$\circ$" denotes algebraic operations, "$+$", "$-$", "$\times$", "$\div$". Here we suppose that $x^{-l} \bmod (x^{2^k}-x) = x^{2^k-1-l}$ for $1 \leq l \leq 2^k-1$ and $x^{1/r} \bmod (x^{2^k}-x) = x^{r^{-1} \bmod (2^k-1)}$ for $\gcd(r, 2^k-1) = 1$. More precisely, for $0 \leq a,u \leq 2^k-1$, we define

$$a \pm_k u = \begin{cases} 2^k-1, & \text{if } a \pm u = 2^k-1, \\ (a \pm u) \bmod (2^k-1), & \text{otherwise,} \end{cases}$$

$$a \times_k u = \begin{cases} 2^k-1, & \text{if } 2^k-1 \mid au \neq 0, \\ au \bmod (2^k-1), & \text{otherwise,} \end{cases}$$

and for $\gcd(u, 2^k-1)=1$,

$$a \div_k u = \begin{cases} 2^k-1, & \text{if } a = 2^k-1, \\ au^{-1} \bmod (2^k-1), & \text{otherwise.} \end{cases}$$

Let

$$\mathcal{W}_e = \{(u,v) | \operatorname{wt}(u)+\operatorname{wt}(v) \le e, 0 \le u \le 2^{n_1}-1, 0 \le v \le 2^{n_2}-1\},$$

$$\overline{\mathcal{W}}_d = \{(a,b) | \operatorname{wt}(a)+\operatorname{wt}(b) \ge d+1, 0 \le a \le 2^{n_1}-1, 0 \le b \le 2^{n_2}-1\}.$$

For $(a,b) \in \mathcal{W}_{n_1+n_2}$ and $(u,v) \in \mathcal{W}_{n_1+n_2}$, $a \circ_{n_1} u$ and $b \circ_{n_2} v$ will be simply denoted by $a \circ u$ and $b \circ v$ respectively if there is no ambiguity; that is, the monomial $x^{a \circ t}$ and the monomial $y^{b \circ v}$ are considered as $x^{a \circ u} \bmod (x^{2^{n_1}}-x)$ and $y^{b \circ v} \bmod (y^{2^{n_2}}-y)$ respectively.

Let f, g, h be (n_1+n_2)-variable functions and g be a function of algebraic degree at most e satisfying that $h=gf$ has algebraic degree at most d, where $n_1 \le n_2$, $e < \frac{n_1+n_2}{2}$ and $e \le d$. Let

$$f(x,y) = \sum_{i=0}^{2^{n_1}-1} \sum_{j=0}^{2^{n_2}-1} f_{ij} x^i y^j, \ f_{ij} \in \mathbb{F}_{2^{\operatorname{lcm}(n_1,n_2)}},$$

$$g(x,y) = \sum_{(i,j) \in \mathcal{W}_e} g_{ij} x^i y^j, \ g_{ij} \in \mathbb{F}_{2^{\operatorname{lcm}(n_1,n_2)}},$$

and

$$h(x,y) = \sum_{(i,j) \in \mathcal{W}_d} h_{ij} x^i y^j, \ h_{ij} \in \mathbb{F}_{2^{\operatorname{lcm}(n_1,n_2)}}$$

be the bivariate polynomial representations of f, g and h respectively. For $(a,b) \in \overline{\mathcal{W}}_d$, we have $h_{a,b}=0$ and thus

$$0 = h_{a,b} = \sum_{(u,v) \in \mathcal{W}_e} \lambda^f_{(a,b),(u,v)} g_{u,v}, \tag{8}$$

where $(a,b) \neq (u,v)$ (since $\mathcal{W}_e \cap \overline{\mathcal{W}}_d = \emptyset$ for $e \le d$) and

$$\lambda^f_{(a,b),(u,v)} = \begin{cases} 0, & \text{if } a=0, u \neq 0 \text{ or } b=0, v \neq 0, \\ f_{0,b-v} + f_{2^{n_1}-1,b-v}, & \text{if } a=u \neq 0, b \neq 0, b \neq v, \\ f_{a-u,0} + f_{a-u,2^{n_2}-1}, & \text{if } a \neq 0, a \neq u, b=v \neq 0, \\ f_{a-u,b-v}, & \text{otherwise.} \end{cases} \tag{9}$$

The system of Equations (8) on $g_{u,v}$'s is homogeneous linear. Denote by $B(f;e,d)$ the coefficient matrix of the equations, that is,

$$B(f;e,d) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b) \in \overline{\mathcal{W}}_d \\ (u,v) \in \mathcal{W}_e}}.$$

The size of the matrix is $\sum_{i=d+1}^{n_1+n_2} \binom{n_1+n_2}{i} \times \sum_{i=0}^{e} \binom{n_1+n_2}{i}$.

An example of the matrix $B(f;e,d)$ is listed in Appendix A.

Theorem 2 *Let $f \in \mathbf{B}_{n_1+n_2}$, $n_1 \le n_2$, $e < \frac{n_1+n_2}{2}$ and $e \le d$. Then there exists no nonzero function g of degree at most e such that the product gf has degree at most d if and only if the matrix $B(f;e,d)$ has full column rank.*

Proof. If the matrix $B(f;e,d)$ has full column rank, i.e., the rank of $B(f;e,d)$ equals the number of $g_{u,v}$'s, then Equations (8) has no nonzero solution and thus f admits no nonzero function g of algebraic degree at most e such that $h=gf$ has algebraic degree at most d.

To prove the "only if" direction of the theorem, we need to show that if the matrix $B(f;e,d)$ has not full column rank, then there always exists a nonzero Boolean function satisfying Equations (8). If $g(x,y)=\sum_{(u,v)\in\mathcal{W}_e} g_{u,v}x^u y^v$ ($g_{u,v}\in\mathbb{F}_{2^{\mathrm{lcm}(n_1,n_2)}}$) satisfies (8), then

$$0=h_{a,b}^2=\sum_{z\in\mathcal{W}_e}(\lambda^f_{(a,b),(u,v)})^2 g_{u,v}^2=\sum_{(u,v)\in\mathcal{W}_e}\lambda^f_{(2a,2b),(2u,2v)}g_{u,v}^2,\ (a,b)\in\overline{\mathcal{W}}_d, \tag{10}$$

showing that $g^2(x,y)=\sum_{(u,v)\in\mathcal{W}_e} g_{u,v}^2 x^{2u}y^{2v}$ satisfies (10) (noting that $f_{2i,2j}=f_{ij}^2$ and $\mathrm{wt}(2u)=\mathrm{wt}(u)$ and $\mathrm{wt}(2v)=\mathrm{wt}(v)$). Since (8) and (10) are actually the same equations, we can see that if $g(x,y)$ satisfies Equations (8) then $\mathrm{Tr}(g(x,y))$ satisfies Equations (8), where $\mathrm{Tr}(x)=x+x^2+\cdots+x^{2^{n-1}}$. Also it follows that if $g(x,y)$ satisfies Equations (8) then $\beta g(x,y)$ and $\mathrm{Tr}(\beta g(x,y))$ satisfy Equations (8) for any $\beta\in\mathbb{F}_{2^k}$. If $g(x,y)\neq 0$, then there is $c_x,c_y\in\mathbb{F}_{2^k}$ such that $g(c_x,c_y)=c\neq 0$, and there is $\beta\in\mathbb{F}_{2^k}$ such that $\mathrm{Tr}(\beta c)\neq 0$ and thus $\mathrm{Tr}(\beta g(x,y))\neq 0$. Now we can see that $\mathrm{Tr}(\beta g(x))$ is a nonzero Boolean function and satisfies (8). Hence, if $B(f;e,d)$ has not full column rank, then there exists a nonzero solution for (8) and therefore there exists a nonzero Boolean function satisfying (8).

Thus the theorem is obtained. □

Remark 1. The theorem shows that $\mathcal{AI}(f)>e$ if and only if the matrix $B(f;e,e)$ has full column rank (since $\mathcal{AI}(f)>e$ if and only if there exists no nonzero function g of degree at most e such that $h=gf$ has degree at most e). Then $\mathcal{AI}(f)=\lceil\frac{n_1+n_2}{2}\rceil$ if and only if the matrix $B(f;\lceil\frac{n_1+n_2}{2}\rceil-1,\lceil\frac{n_1+n_2}{2}\rceil-1)$ has full column rank.

4 A special class of Boolean functions using bivariate polynomial representation

In this section we study the immunity against fast algebraic attacks of the $2k$-variable Boolean function

$$\tau(x,y)=\phi(xy^r)+(x^{2^k-1}+1)\psi(y)+(y^{2^k-1}+1)\varphi(x), \tag{11}$$

where ϕ, ψ and φ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$, $1\le r\le 2^k-2$ and $\gcd(r,2^k-1)=1$. In Section 4.1 we present the bivariate polynomial representation of the function τ. Then, in Section 4.2, we propose several useful properties of the matrix $B(\tau;e,d)$. In Section 4.3 and Section 4.4 we discuss the immunity of the function τ against fast algebraic attacks.

4.1 The bivariate polynomial representation

Hereinafter, let $\sum_{i=0}^{2^k-1}\phi_i x^i$, $\phi_i\in\mathbb{F}_{2^k}$, be the univariate polynomial representation of $\phi(x)$, and let $\sum_{i=0}^{2^k-1}\sum_{i=0}^{2^k-1}\Phi_{ij}x^iy^j$, $\Phi_{ij}\in\mathbb{F}_{2^k}$, be the bivariate polynomial representation of $\phi(xy^r)$. For $\gcd(r,2^k-1)=1$, it holds that

$$\Phi_{ij}=\begin{cases}\phi_0, & \text{if } i=j=0,\\ \phi_i, & \text{if } 1\le i,j\le 2^k-2 \text{ and } j\equiv ri(\bmod 2^k-1),\\ \phi_{2^k-1}, & \text{if } i=j=2^k-1,\\ 0, & \text{otherwise.}\end{cases} \tag{12}$$

That is, $\Phi_{ij}=\phi_i$ when $j=ri$ and $\Phi_{ij}=0$ when $j\neq ri$, where ri is considered as $r\times_k i$. Then the algebraic degree of $\phi(xy^r)$ is equal to $\max\{\mathrm{wt}(i)+\mathrm{wt}(ri)|\phi_i\neq 0, 0\le i\le 2^k-1\}$ and is thus at least $2k-1-\min\{\mathrm{wt}(r),\mathrm{wt}(r^{-1})\}$ when $\phi_{2^k-2}\neq 0$ and $\phi_{(2^k-2)/r}\neq 0$.

Let $\sum_{j=0}^{2^k-1}\psi_j y^j$ and $\sum_{i=0}^{2^k-1}\varphi_i x^i$ be the univariate polynomial representations of $\psi(y)$ and $\varphi(x)$ respectively, $\psi_j,\varphi_i\in\mathbb{F}_{2^k}$. Let $\sum_{i=0}^{2^k-1}\sum_{i=0}^{2^k-1}\tau_{ij}x^iy^j$ be the bivariate polynomial representation of $\tau(x,y)$.

Then for $\gcd(r, 2^k-1)=1$, we have

$$\tau_{ij}=\begin{cases}\phi_0+\psi_0+\varphi_0, & \text{if } i=j=0,\\ \phi_{2^k-1}+\psi_{2^k-1}+\varphi_{2^k-1}, & \text{if } i=j=2^k-1,\\ \psi_{2^k-1}+\varphi_0, & \text{if } i=0 \text{ and } j=2^k-1,\\ \psi_0+\varphi_{2^k-1}, & \text{if } i=2^k-1 \text{ and } j=0,\\ \psi_j, & \text{if } i\in\{0,2^k-1\} \text{ and } 1\le j\le 2^k-2,\\ \varphi_i, & \text{if } 1\le i\le 2^k-2 \text{ and } j\in\{0,2^k-1\},\\ \phi_i, & \text{if } 1\le i,j\le 2^k-2 \text{ and } j\equiv ri(\bmod 2^k-1),\\ 0, & \text{otherwise.}\end{cases} \tag{13}$$

We assume without loss of generality that $\psi_{2^k-1}=\varphi_{2^k-1}=0$ (since the other cases are included into this case). Note that the constant term τ_{00} does not affect the immunity against fast algebraic attacks. Assume without loss of generality that $\phi_0+\psi_0+\varphi_0=0$. Then for the function τ, we have

$$\tau_{ij}=\begin{cases}\varphi_0, & \text{if } i=0 \text{ and } j=2^k-1,\\ \psi_0, & \text{if } i=2^k-1 \text{ and } j=0,\\ \psi_j, & \text{if } i\in\{0,2^k-1\} \text{ and } 1\le j\le 2^k-2,\\ \varphi_i, & \text{if } 1\le i\le 2^k-2 \text{ and } j\in\{0,2^k-1\},\\ \phi_i, & \text{if } 1\le i,j\le 2^k-1 \text{ and } j\equiv ri(\bmod 2^k-1),\\ 0, & \text{otherwise.}\end{cases} \tag{14}$$

In this case, we can see that the algebraic degree of τ is equal to $\max\{\deg(\phi(xy^r)),\deg(\psi)+k,\deg(\varphi)+k\}$ and is thus equal to $2k-1$ when $\deg(\phi)<k$ and $\max\{\deg(\psi),\deg(\varphi)\}=k-1$.

4.2 Properties of $B(\tau;e,d)$

In this section we study the properties of the matrix $B(\tau;e,d)$. The results of this section will be useful in Section 4.3 and Section 5.

Hereinafter we consider $n_1=n_2=k$ and denote

$$\mathcal{W}_e=\{(u,v)|\,\mathrm{wt}(u)+\mathrm{wt}(v)\le e, 0\le u,v\le 2^k-1\},$$

$$\overline{\mathcal{W}}_d=\{(a,b)|\,\mathrm{wt}(a)+\mathrm{wt}(b)\ge d+1, 0\le a,b\le 2^k-1\},$$

$$\mathcal{W}_e^*=\{(u,v)\in\mathcal{W}_e|1\le u,v\le 2^k-2\},$$

$$\overline{\mathcal{W}}_d^*=\{(a,b)\in\overline{\mathcal{W}}_d|1\le a,b\le 2^k-2\}.$$

For $0\le t\le 2^k-2$, let

$$\mathcal{W}_{e,r,t}=\{(u,v)\in\mathcal{W}_e|v-ru\equiv t(\bmod 2^k-1)\}, \tag{15}$$

$$\overline{\mathcal{W}}_{d,r,t}=\{(a,b)\in\overline{\mathcal{W}}_d|b-ra\equiv t(\bmod 2^k-1)\}. \tag{16}$$

Let

$$\mathcal{W}_{e,r,0}^*=\mathcal{W}_{e,r,0}\setminus\{(0,0)\}, \tag{17}$$

$$\overline{\mathcal{W}}_{d,r,0}^*=\overline{\mathcal{W}}_{d,r,0}\setminus\{(2^k-1,0),(0,2^k-1),(2^k-1,2^k-1)\}, \tag{18}$$

and for $1\le t\le 2^k-2$, let

$$\mathcal{W}_{e,r,t}^*=\mathcal{W}_{e,r,t}\setminus\{(0,t),(-r^{-1}t,0)\}, \tag{19}$$

$$\overline{\mathcal{W}}_{d,r,t}^*=\overline{\mathcal{W}}_{d,r,t}\setminus\{(0,t),(-r^{-1}t,0),(2^k-1,t),(-r^{-1}t,2^k-1)\}. \tag{20}$$

By (15), (17) and (19), it holds for $e\le k-1$ that

$$\mathcal{W}_{e,r,t}^*=\mathcal{W}_{e,r,t}\setminus\{(u,v)|u\in\{0,2^k-1\} \text{ or } v\in\{0,2^k-1\}\}$$

and thus $\mathcal{W}^*_{e,r,t} \subset \mathcal{W}^*_e$. By (16), (18) and (20), it holds that

$$\overline{\mathcal{W}}^*_{d,r,t} = \overline{\mathcal{W}}_{d,r,t} \setminus \{(a,b) | a \in \{0, 2^k - 1\} \text{ or } b \in \{0, 2^k - 1\}\}$$

and thus $\overline{\mathcal{W}}^*_{d,r,t} \subset \overline{\mathcal{W}}^*_d$. In particular, if $d \geq k-1$, then $\overline{\mathcal{W}}^*_{d,r,t} = \overline{\mathcal{W}}_{d,r,t} \setminus \{(2^k-1, t), (-r^{-1}t, 2^k-1)\}$ for $t \neq 0$; if $d \geq k$, then $\overline{\mathcal{W}}^*_{d,r,0} = \overline{\mathcal{W}}_{d,r,0} \setminus \{(2^k-1, 2^k-1)\}$.

Denote by $B_*(f; e, d)$ the matrix formed by selecting columns (u, v) with $(u, v) \in \mathcal{W}^*_e$ from $B(f; e, d)$, that is,

$$B_*(f; e, d) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}_d \\ (u,v)\in\mathcal{W}^*_e}}.$$

Denote by $B^*(f; e, d)$ the matrix obtained by selecting rows (a, b) with $(a, b) \in \overline{\mathcal{W}}^*_d$ from $B(f; e, d)$, that is,

$$B^*(f; e, d) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}^*_d \\ (u,v)\in\mathcal{W}_e}}.$$

It is clear that $B_*(f; e, d)$ and $B^*(f; e, d)$ are submatrices of $B(f; e, d)$.

Let $B(f; e, d; r, t)$ be the submatrix of $B(f; e, d)$ formed by selecting rows (a, b) and columns (u, v) with $(a, b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u, v) \in \mathcal{W}_{e,r,t}$, that is,

$$B(f; e, d; r, t) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}_{d,r,t} \\ (u,v)\in\mathcal{W}_{e,r,t}}}.$$

We can see that $B(f; e, d; r, t)$ is a $\#\overline{\mathcal{W}}_{d,r,t} \times \#\mathcal{W}_{e,r,t}$ matrix, where $\#$ denotes the number of elements in a set. The matrix $B(f; e, d; r, t)$ is conventionally considered as a full column rank matrix when $\#\mathcal{W}_{e,r,t} = 0$.

Let $B_*(f; e, d; r, t)$ be the matrix formed by removing columns $(0, t)$ and $(-r^{-1}t, 0)$, if any, from $B(f; e, d; r, t)$, that is,

$$B_*(f; e, d; r, t) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}_{d,r,t} \\ (u,v)\in\mathcal{W}^*_{e,r,t}}}.$$

Let $B^*(f; e, d; r, t)$ be the matrix formed by removing rows $(0, t)$, $(-r^{-1}t, 0)$, $(2^k-1, t)$, $(-r^{-1}t, 2^k-1)$ and $(2^k-1, 2^k-1)$, if any, from $B(f; e, d; r, t)$, that is,

$$B^*(f; e, d; r, t) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}^*_{d,r,t} \\ (u,v)\in\mathcal{W}_{e,r,t}}}.$$

It is clear that $B_*(f; e, d; r, t)$ and $B^*(f; e, d; r, t)$ are submatrices of $B(f; e, d; r, t)$. Since $\mathcal{W}^*_{e,r,t} \subset \mathcal{W}^*_e$, $B_*(f; e, d; r, t)$ is a submatrix of $B_*(f; e, d)$; since $\overline{\mathcal{W}}^*_{d,r,t} \subset \overline{\mathcal{W}}^*_d$, $B^*(f; e, d; r, t)$ is a submatrix of $B^*(f; e, d)$.

Next we discuss the matrix $B_*(\tau; e, d)$.

Proposition 3 *$B_*(\tau; e, d) = B_*(\phi(xy^r); e, d)$ and $B_*(\tau; e, d; r, t) = B_*(\phi(xy^r); e, d; r, t)$.*

Proof. We just prove $B_*(\tau; e, d) = B_*(\phi(xy^r); e, d)$. For $(u, v) \in \mathcal{W}^*_e$ and $(a, b) \in \overline{\mathcal{W}}_d$ with $a = u$, we have $v \neq 0$, $b - v \neq 2^k - 1$, and thus $\lambda^\tau_{(a,b),(u,v)} = \psi_{b-v} + \psi_{b-v} = 0$ by (9) and (14); by (9) and (12) we also have $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = 0$. For $(u, v) \in \mathcal{W}^*_e$ and $(a, b) \in \overline{\mathcal{W}}_d$ with $b = v$, we similarly have $\lambda^\tau_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)} = 0$. For $(u, v) \in \mathcal{W}^*_e$ and $(a, b) \in \overline{\mathcal{W}}_d$ with $a \neq u$ and $b \neq v$, we have $u \neq 0$ and $v \neq 0$, and thus $\lambda^\tau_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \phi_{a-u}$ by (9), (14) and (12). Then $\lambda^\tau_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)}$ for $(u, v) \in \mathcal{W}^*_e$ and $(a, b) \in \overline{\mathcal{W}}_d$. Thus $B_*(\tau; e, d) = B_*(\phi(xy^r); e, d)$. □

Next we discuss the matrix $B^*(\tau; e, d)$.

Proposition 4 *$B^*(\tau; e, d) = B^*(\phi(xy^r); e, d)$ and $B^*(\tau; e, d; r, t) = B^*(\phi(xy^r); e, d; r, t)$.*

Proof. We just prove $B^*(\tau;e,d) = B^*(\phi(xy^r);e,d)$. For $(u,v) \in \mathcal{W}_e$ and $(a,b) \in \overline{\mathcal{W}}_d^*$ with $a = u$, we have $b \neq 2^k-1$, $b-v \neq 2^k-1$ and thus $\lambda^{\tau}_{(a,b),(u,v)} = \psi_{b-v} + \psi_{b-v} = 0$ by (9) and (14); by (9) and (12) we also have $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = 0$. For $(u,v) \in \mathcal{W}_e$ and $(a,b) \in \overline{\mathcal{W}}_d^*$ with $b = v$, we similarly have $\lambda^{\tau}_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)} = 0$. For $(u,v) \in \mathcal{W}_e$ and $(a,b) \in \overline{\mathcal{W}}_d^*$, we have $a \neq 0$, $a \neq 2^k-1$, $b \neq 0$ and $b \neq 2^k-1$, and thus $\lambda^{\tau}_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \phi_{a-u}$ by (9), (14) and (12). Thus $B^*(\tau;e,d) = B^*(\phi(xy^r);e,d)$. □

From the above results, the matrix $B(\tau;e,d)$ is very close to the matrix $B(\phi(xy^r);e,d)$. The question whether the matrix $B(\tau;e,d)$ has full column rank is highly depended on whether $B_*(\phi(xy^r);e,d)$ and $B^*(\phi(xy^r);e,d)$ have full column rank. Since $B_*(\phi(xy^r);e,d)$ is a collect of column vectors of $B(\tau;e,d)$, as described in (2), if $B_*(\phi(xy^r);e,d)$ has not full column rank, then $B(\tau;e,d)$ also has not full column rank; while $B^*(\phi(xy^r);e,d)$ is a collect of row vectors of $B(\tau;e,d)$, as described in (1), if $B^*(\phi(xy^r);e,d)$ has full column rank, then $B(\tau;e,d)$ also has full column rank.

Since $B(\phi(xy^r);e,d)$ is a quasidiagonal matrix (see Proposition 8), $B_*(\phi(xy^r);e,d)$ and $B^*(\phi(xy^r);e,d)$ are also quasidiagonal matrices. Then the question whether the matrix $B(\tau;e,d)$ has full column rank might be simplified to the questions whether all the matrices $B_*(\phi(xy^r);e,d;r,t)$ have full column rank and whether all the matrices $B^*(\phi(xy^r);e,d;r,t)$ have full column rank. Further, by Proposition 5 it only needs to consider one matrix among the matrices $B(\phi(xy^r);e,d;r,2^st)$ with $0 \leq s \leq k-1$.

Next we discuss the matrix $B(\tau;e,d;r,t)$. The following result applies to any $2k$-variable function $f(x,y)$.

Proposition 5 *For $0 \leq t \leq 2^k-2$, $\#\overline{\mathcal{W}}_{d,r,2t} = \#\overline{\mathcal{W}}_{d,r,t}$ and $\#\mathcal{W}_{e,r,2t} = \#\mathcal{W}_{e,r,t}$; $B(f;e,d;r,2t)$ has full column rank if and only if $B(f;e,d;r,t)$ has full column rank.*

Proof. Since $\mathrm{wt}(2a) = \mathrm{wt}(a)$, $\mathrm{wt}(2b) = \mathrm{wt}(b)$, and $b - ra \equiv t \pmod{2^k-1}$ if and only if $2b - 2ra \equiv 2t \pmod{2^k-1}$, we have $\#\overline{\mathcal{W}}_{d,r,2t} = \#\overline{\mathcal{W}}_{d,r,t}$ and $\#\mathcal{W}_{e,r,2t} = \#\mathcal{W}_{e,r,t}$ for $0 \leq t \leq 2^k-2$. From (6) and (9) we know that the element at row $(2a,2b)$ and column $(2u,2v)$ of $B(f;e,d;r,2t)$ is the square of the element at row (a,b) and column (u,v) of $B(f;e,d;r,t)$. Since the elements of the two matrices are in fields with characteristic 2, they have the same rank. Thus, $B(f;e,d;r,2t)$ has full column rank if and only if $B(f;e,d;r,t)$ has full column rank. □

Proposition 6 *Let $(r,2^k-1) = 1$, $e \leq k-1$ and $e \leq d$. Then the rank of $B(\tau;e,d;r,0)$ is greater than or equal to the rank of $B(\phi(xy^r);e,d;r,0)$. Further, if $k \leq d$, then*

$$B(\tau;e,d;r,0) = B(\phi(xy^r);e,d;r,0) = (\phi_{a-u})_{\substack{a\in\mathcal{A}\\ u\in\mathcal{U}}},$$

where

$$\mathcal{A} = \{a|\, \mathrm{wt}(a) + \mathrm{wt}(ra) \geq d+1, 1 \leq a \leq 2^k-1\},$$
$$\mathcal{U} = \{u|\, \mathrm{wt}(u) + \mathrm{wt}(ru) \leq e, 0 \leq u \leq 2^k-2\}.$$

Proof. By (15) and (16) we have

$$\mathcal{W}_{e,r,0} = \{(u,v)|\, \mathrm{wt}(u) + \mathrm{wt}(v) \leq e, v \equiv ru \pmod{2^k-1}, 0 \leq u,v \leq 2^k-2\},$$
$$\overline{\mathcal{W}}_{d,r,0} = \{(a,b)|\, \mathrm{wt}(a) + \mathrm{wt}(b) \geq d+1, b \equiv ra \pmod{2^k-1}, 0 \leq a,b \leq 2^k-1\}.$$

and $\mathcal{W}_{e,r,0}$ and $\overline{\mathcal{W}}_{d,r,0}$ are disjoint for $e \leq d$. Let $(a,b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$. When $a \neq 0$, we have $a \neq u$ (if $a = u$ then $b = 2^k-1$ and $v = 0$, and thus $a = u \equiv 0 \pmod{2^k-1}$, which is impossible); when $a = u = 0$, we have $b = 2^k-1$ and $v = 0$. Similarly, when $b \neq 0$, we have $b \neq v$; when $b = v = 0$, we have $a = 2^k-1$ and $u = 0$. Therefore, when $(a,b) \neq (0,2^k-1)$ and $(a,b) \neq (2^k-1,0)$, by (9) we have $\lambda^{\tau}_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)} = 0$ or $\lambda^{\tau}_{(a,b),(u,v)} = \tau_{a-u,b-v}$ and $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \Phi_{a-u,b-v}$, where $a \neq u$, $b \neq v$ and $b - v \equiv r(a-u) \pmod{2^k-1}$. Then we obtain $\tau_{a-u,b-v} = \phi_{a-u}$ by (14) and $\Phi_{a-u,b-v} = \phi_{a-u}$ by (12).

We can see that $\lambda^{\tau}_{(a,b),(u,v)} = \lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \phi_{a-u}$ when $(a,b) \neq (0,2^k-1)$ and $(a,b) \neq (2^k-1,0)$. For $(a,b) = (0,2^k-1)$ or $(2^k-1,0)$, we have $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = 0$ by (9) and by (12). Thus the rank of $B(\tau;e,d;r,0)$ is greater than or equal to the rank of $B(\phi(xy^r);e,d;r,0)$.

For $d \geq k$, we have $(a,b) \neq (0,2^k-1)$ and $(a,b) \neq (2^k-1,0)$ for $(a,b) \in \overline{\mathcal{W}}_{d,r,0}$. Thus $B(\tau;e,d;r,0) = B(\phi(xy^r);e,d;r,0)$. From the above proof, we can obtain that

$$\mathcal{A} = \{a | \operatorname{wt}(a) + \operatorname{wt}(ra) \geq d+1, 1 \leq a \leq 2^k-1\},$$

$$\mathcal{U} = \{u | \operatorname{wt}(u) + \operatorname{wt}(ru) \leq e, 0 \leq u \leq 2^k-2\}.$$

Hence we have proven the proposition. □

Proposition 7 *Let $(r, 2^k-1) = 1$. Then $\#\overline{\mathcal{W}}_{2k-e-1,r,0} = \#\mathcal{W}_{e,r,0}$ and $\#\overline{\mathcal{W}}_{d,r,0} \geq \#\mathcal{W}_{e,r,0}$ for $d \leq 2k-e-1$.*

Proof. Since $\#\overline{\mathcal{W}}_{d,r,0}$ increases as d decreases, it just needs to prove $\#\overline{\mathcal{W}}_{2k-e-1,r,0} = \#\mathcal{W}_{e,r,0}$. Let $0 \leq a \leq 2^k-1$ and $u = 2^k-1-a$. Since

$$\operatorname{wt}(u) + \operatorname{wt}(ur) = \operatorname{wt}(2^k-1-a) + \operatorname{wt}(2^k-1-ar) = 2k - (\operatorname{wt}(a) + \operatorname{wt}(ar)),$$

we know that $\operatorname{wt}(a) + \operatorname{wt}(ar) \geq 2k-e$ if and only if $\operatorname{wt}(u) + \operatorname{wt}(ur) \leq e$. Then by (15) and (16) we have $\#\overline{\mathcal{W}}_{2k-e-1,r,0} = \#\mathcal{W}_{e,r,0}$. □

Taking $e = d = k-1$, the result shows that $\#\mathcal{W}_{k-1,r,0} \leq 2^{k-1}$.

Then we discuss the matrix $B(\phi(xy^r);e,d)$ and $B(\phi(xy^r);e,d;r,t)$.

Proposition 8 *The rank of $B(\phi(xy^r);e,d)$ equals the sum of ranks of $B(\phi(xy^r);e,d;r,t)$ over all t with $0 \leq t \leq 2^k-2$.*

Proof. From (12) we know $\Phi_{ij} \neq 0$ only when $j \equiv ri (\bmod 2^k-1)$. Then from (9) we know $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} \neq 0$ only when $b-v \equiv r(a-u) (\bmod 2^k-1)$. In other words, $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} \neq 0$ only when $b-ra \equiv v-ru \equiv t (\bmod 2^k-1)$, $0 \leq t \leq 2^k-2$. Therefore, the matrix $B(\phi(xy^r);e,d)$ is a quasidiagonal matrix as

$$\begin{pmatrix} B(\phi(xy^r);e,d;r,0) & 0 & \cdots & 0 \\ 0 & B(\phi(xy^r);e,d;r,1) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B(\phi(xy^r);e,d;r,2^k-2) \end{pmatrix}.$$

Then the rank of $B(\phi(xy^r);e,d)$ equals the sum of ranks of $B(\phi(xy^r);e,d;r,t)$ over all t with $0 \leq t \leq 2^k-2$. □

Now we discuss the matrix $B(\phi(xy^r);e,d;r,t)$.

For $(a,b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$, when $a = u$, by (15) and (16) we have $b = 2^k-1$ and $v = 0$ (since $(a,b) \neq (u,v)$), and thus $a = u = -r^{-1}t \bmod (2^k-1)$, which shows that for $d+1-k \leq \operatorname{wt}(-r^{-1}t) \leq e$, $a = u$ if and only if $(a,b) = (-r^{-1}t, 2^k-1)$ and $(u,v) = (-r^{-1}t, 0)$; for the other cases, there exist no $(a,b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$ such that $a = u$. Similarly, for $d+1-k \leq \operatorname{wt}(t) \leq e$, $b = v$ if and only if $(a,b) = (2^k-1,t)$ and $(u,v) = (0,t)$; for the other cases, there exist no $(a,b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$ such that $b = v$.

Therefore, for $(a,b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$, where $e \leq d$ and $0 \leq t \leq 2^k-2$, from (9) we have

$$\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \begin{cases} 0, & \text{if } a = 0, u \neq 0 \text{ or } b = 0, v \neq 0, \\ \Phi_{0,2^k-1} + \Phi_{2^k-1,2^k-1}, & \text{if } (a,b) = (-r^{-1}t, 2^k-1), (u,v) = (-r^{-1}t, 0), \\ \Phi_{2^k-1,0} + \Phi_{2^k-1,2^k-1}, & \text{if } (a,b) = (2^k-1,t), (u,v) = (0,t), \\ \Phi_{a-u,b-v}, & \text{if } a \neq 0, a \neq u, b \neq 0, b \neq v, \end{cases} \tag{21}$$

where $b - v \equiv r(a-u) (\mathrm{mod}\, 2^k - 1)$, and by (12) we then have

$$\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \begin{cases} 0, & \text{if } a = 0, u \neq 0 \text{ or } b = 0, v \neq 0, \\ \phi_{2^k-1}, & \text{if } (a,b) = (-r^{-1}t, 2^k-1), (u,v) = (-r^{-1}t, 0), \\ \phi_{2^k-1}, & \text{if } (a,b) = (2^k-1, t), (u,v) = (0,t), \\ \phi_{2^k-1}, & \text{if } (a,b) = (2^k-1, 2^k-1), (u,v) = (0,0), \\ \phi_{a-u}, & \text{if } a \neq 0, b \neq 0, a-u \notin \{0, 2^k-1\}, \end{cases} \tag{22}$$

As mentioned above, if $k + e \leq d$, then we have $a \neq 0, b \neq 0$ and $a - u \notin \{0, 2^k - 1\}$ for $(a, b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u, v) \in \mathcal{W}_{e,r,t}$ with $1 \leq t \leq 2^k - 2$ (since $(2^k - 1, 2^k - 1) \in \overline{\mathcal{W}}_{d,r,0}$).

Proposition 9 *Let $k+e \leq d$ and $1 \leq t \leq 2^k-2$. Then for $(a,b) \in \overline{\mathcal{W}}_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$, $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \phi_{a-u}$ and $a - u \notin \{0, 2^k - 1\}$.*

Form (22) we can see that $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \phi_{a-u}$ and $a-u \notin \{0, 2^k-1\}$ for $(a,b) \in \overline{\mathcal{W}}^*_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$.

Proposition 10 *For $(a,b) \in \overline{\mathcal{W}}^*_{d,r,t}$ and $(u,v) \in \mathcal{W}_{e,r,t}$, $\lambda^{\phi(xy^r)}_{(a,b),(u,v)} = \phi_{a-u}$ and $a - u \notin \{0, 2^k - 1\}$.*

4.3 The immunity against fast algebraic attacks

First we study the immunity of the $2k$-variable Boolean functions $\phi(xy^r)$ against fast algebraic attacks.

Theorem 11 *Let $\phi \in \mathbf{B}_k$ and $(r, 2^k - 1) = 1$. Then there exists no nonzero function $g \in \mathbf{B}_{2k}$ of degree at most e such that the product $g(x,y)\phi(xy^r)$ has degree at most d if and only if all the matrices $B(\phi(xy^r); e, d; r, t)$, $0 \leq t \leq 2^k - 2$, have full column rank.*

Proof. Proposition 8 shows that $B(\phi(xy^r); e, d)$ has full column rank if and only if all the matrices $B(\phi(xy^r); e, d; r, t)$, $0 \leq t \leq 2^k - 2$, have full column rank. Then the theorem is derived from Theorem 2. □

Remark 2. Theorem 11 shows that $\mathcal{AI}(\phi(xy^r)) > e$ if and only if all the matrices $B(\phi(xy^r); e, e; r, t)$, $0 \leq t \leq 2^k - 2$, have full column rank; in particular, $\mathcal{AI}(\phi(xy^r)) = k$ if and only if all the matrices $B(\phi(xy^r); k-1, k-1; r, t)$, $0 \leq t \leq 2^k - 2$, have full column rank.

Corollary 12 *Let $\phi \in \mathbf{B}_k$ and $(r, 2^k-1) = 1$. If there is t with $0 \leq t \leq 2^k-2$ such that $\#\overline{\mathcal{W}}_{d,r,t} < \#\mathcal{W}_{e,r,t}$, then there exists a nonzero function $g \in \mathbf{B}_{2k}$ with degree at most e such that the product $g(x,y)\phi(xy^r)$ has degree at most d.*

Proof. It is derived from Theorem 11 since $B(\phi(xy^r); e, d; r, t)$ is a $\#\overline{\mathcal{W}}_{d,r,t} \times \#\mathcal{W}_{e,r,t}$ matrix. □

Remark 3. Proposition 7 has shown that $\#\overline{\mathcal{W}}_{d,r,0} \geq \#\mathcal{W}_{e,r,0}$ for $d \leq 2k - e - 1$, so we can ignore the case $t = 0$. Corollary 12 shows that if $\mathcal{AI}(f) > e$ then $\#\mathcal{W}_{e,r,t} \leq 2^{k-1}$ for $1 \leq t \leq 2^k - 2$; in particular, if $\mathcal{AI}(f) = k$ then $\#\mathcal{W}_{k-1,r,t} \leq 2^{k-1}$ for $1 \leq t \leq 2^k - 2$. This implies that Tu-Deng function, which belongs to the family of $\phi(xy^{2^k-2})$, has maximum $\mathcal{AI}$ if and only if Tu-Deng conjecture is correct (since it was proven in [22] that if Tu-Deng conjecture is correct then Tu-Deng function has maximum $\mathcal{AI}$). A similar result also applies to the relationship between Jin et al.'s functions and the related conjectures [13].

Then we study the immunity against fast algebraic attacks of the $2k$-variable Boolean functions $\tau(x, y)$ described in (11).

A trivial observation is that there always exists a nonzero quadratic function g such that the product $g\tau$ has algebraic degree at most $\deg(\phi(xy^r))+2$, e.g., $g(x, y) = xy$. Also there always exists a nonzero affine function g such that the product $g(x, y)(\phi(xy^r) + (x^{2^k-1} + 1)\psi(y))$ has degree at most $\deg(\phi(xy^r)) + 1$, e.g., $g(x, y) = x$; a similar result applies to $\phi(xy^r) + (y^{2^k-1} + 1)\varphi(x)$. The family of the functions τ with $\deg(\phi) < k$ and $r = 2^k - 2$, including the family of Tu-Deng functions [22], are weak against fast algebraic attacks, since the algebraic degree of $\phi(xy^{2^k-2})$ is less than or equal to k when $\deg(\phi) < k$.

Theorem 13 *If there is t, $0 \le t \le 2^k-2$, such that $B_*(\phi(xy^r);e,d;r,t)$ has not full column rank, then there exists a nonzero function g with degree at most e such that the product $g\tau$ has degree at most d.*

Proof. The same proof of Proposition 8 shows that $B_*(\phi(xy^r);e,d)$ has not full column rank if $B_*(\phi(xy^r);e,d;r,t)$ has not full column rank. Then, by Proposition 3, $B_*(\tau;e,d)$ and $B(\tau;e,d)$ have not full column rank. The theorem is therefore derived from Theorem 2. □

Corollary 14 *If there is t, $0 \le t \le 2^k-2$, such that $\#\overline{\mathcal{W}}_{d,r,t} < \#\mathcal{W}^*_{e,r,t}$, then there exists a nonzero function g with degree at most e such that the product $g\tau$ has degree at most d.*

Proof. It is derived from Theorem 13 since $B^*(\tau;e,d;r,t)$ is a $\#\overline{\mathcal{W}}_{d,r,t} \times \#\mathcal{W}^*_{e,r,t}$ matrix. □

Similar results of Theorem 13 and Corollary 14 apply to the functions $\phi(xy^r)+(x^{2^k-1}+1)\psi(y)$ and $\phi(xy^r)+(y^{2^k-1}+1)\varphi(x)$ when the set $\mathcal{W}^*_{e,r,t}$ is replaced with $\mathcal{W}_{e,r,t}\setminus\{(0,t)\}$ and $\mathcal{W}_{e,r,t}\setminus\{(-r^{-1}t,0)\}$ respectively.

For $0 \le t \le 2^k-2$, denote

$$\overline{\mathcal{W}}^+_{d,r,t} = \overline{\mathcal{W}}_{d,r,t} \cup \{(a,b)\in\overline{\mathcal{W}}_d | a\in\{0,2^k-1\} \text{ or } b\in\{0,2^k-1\}\} = \overline{\mathcal{W}}_d \setminus (\bigcup_{t^*\neq t} \overline{\mathcal{W}}^*_{d,r,t^*})$$

and

$$B^+(f;e,d;r,t) = \left(\lambda^f_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}^+_{d,r,t}\\(u,v)\in\mathcal{W}_{e,r,t}}}.$$

Theorem 15 *Let $e \le d$ and $0 \le t \le 2^k-2$. If $B^+(\tau;e,d;r,t)$ and all the matrices $B^*(\phi(xy^r);e,d;r,t^*)$, $0 \le t^* \le 2^k-2$ and $t^* \neq t$, have full column rank, then there exists no nonzero function g of degree at most e such that the product $g\tau$ has degree at most d.*

Proof. Proposition 8 and Proposition 4 state that after appropriate matrix transformations the matrix $B(\tau;e,d)$ can be represented as

$$\begin{pmatrix} * & * & \cdots & * \\ B^*(\phi(xy^r);e,d;r,0) & 0 & \cdots & 0 \\ 0 & B^*(\phi(xy^r);e,d;r,1) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B^*(\phi(xy^r);e,d;r,2^k-2) \end{pmatrix}.$$

Assume without loss of generality that $t=0$. If all the matrices $B^*(\phi(xy^r);e,d;r,t^*)$, $1 \le t^* \le 2^k-2$, have full column rank, then $B(\tau;e,d)$ has full column rank if and only if $B^+(\tau;e,d;r,0)$ has full column rank. The theorem is thus derived from Theorem 2. □

Corollary 16 *Let $e \le d$. If $B(\phi(xy^r);e,d;r,0)$ and all the matrices $B^*(\phi(xy^r);e,d;r,t)$, $1 \le t \le 2^k-2$, have full column rank, then there exists no nonzero function g of degree at most e such that the product $g\tau$ has degree at most d.*

Proof. By Proposition 6 we know $B(\tau;e,d;r,0) = B(\phi(xy^r);e,d;r,0)$. Then the result is derived from Theorem 15. □

Corollary 17 *Let $e \le d$. If all the matrices $B^*(\phi(xy^r);e,d;r,t)$, $0 \le t \le 2^k-2$, have full column rank, then there exists no nonzero function g of degree at most e such that the product $g\tau$ has degree at most d.*

Proof. It is derived from Theorem 15. □

From the results presented in this section, we obtain an efficient method for computing the immunity of the function τ against fast algebraic attacks (see Appendix D). The sizes of the matrices we need to compute in this section are much smaller than that of $B(\tau;e,d)$. When ϕ is a special function, e.g., Carlet-Feng function [4], our method could become more powerful (see Appendix E).

4.4 The immunity against fast algebraic attacks for the case $r = 1$

Next we study the immunity against fast algebraic attacks of the $2k$-variable Boolean functions τ for $r = 1$, that is,

$$\tau(x, y) = \phi(xy) + (x^{2^k-1} + 1)\psi(y) + (y^{2^k-1} + 1)\varphi(x), \tag{23}$$

where ϕ, ψ and φ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$. It is clear that the algebraic degree of $\phi(xy)$ is $2\deg(\phi)$.

Theorem 18 *Let $r = 1$ and $d = \max\{2k - 2e - 2, k + \deg(\psi), k + \deg(\varphi)\}$.*

If $\deg(\phi) < k$, then for $e < k/2$ such that $\binom{k-1}{e} \equiv 1 (\mathrm{mod}\, 2)$, there exists a nonzero function g with degree at most $2e$ such that the product $g\tau$ has degree at most d. Further, if $k \neq 2^s + 1$ and $\deg(\phi) < k$, then there exist a positive integer $e < k/2$ and a nonzero function g with degree at most $2e$ such that the product $g\tau$ has degree at most d.

If $\deg(\phi) = k$, then for $e < k/2$ such that $\binom{k-1}{e} \equiv 0 (\mathrm{mod}\, 2)$, there exists a nonzero function g with degree at most $2e$ such that the product $g\tau$ has degree at most d. Further, if $k \neq 2^s$ and $\deg(\phi) = k$, then there exist a positive integer $e < k/2$ and a nonzero function g with degree at most $2e$ such that the product $g\tau$ has degree at most d.

Proof. We just prove the first half part of the theorem (the second half part can be similarly obtained). By Theorem 1 we know that if $\deg(\phi) < k$, then for $e < k/2$ such that $\binom{k-1}{e} \equiv 1 (\mathrm{mod}\, 2)$, there exists a nonzero function $g^* \in \mathbf{B}_k$ with degree at most e such that the product $g^*(xy)\phi(xy)$ has degree at most $2(k - e - 1)$. Let $g(x, y) = g^*(xy)$ then g has degree at most $2e$ and

$$\begin{aligned} g(x, y)\tau(x, y) =& g^*(xy)\phi(xy) + g^*(xy)(x^{2^k-1} + 1)\psi(y) + g^*(xy)(y^{2^k-1} + 1)\varphi(x) \\ =& g^*(xy)\phi(xy) + g^*(0)(x^{2^k-1} + 1)\psi(y) + g^*(0)(y^{2^k-1} + 1)\varphi(x). \end{aligned}$$

Thus $g\tau$ has degree at most d. Further, if $k \neq 2^s + 1$, then, by Lucas' theorem, there always exists a positive integer $e < k/2$ such that $\binom{k-1}{e} \equiv 1 (\mathrm{mod}\, 2)$. Hence the first half part of the theorem has been proven. □

The theorem shows that for $k \neq 2^s$ and $k \neq 2^s + 1$ and $r = 1$, if both $\deg(\psi)$ and $\deg(\varphi)$ are reasonable small, then there exists a nonzero function g with degree at most $2e$ ($e < k/2$) such that the product $g\tau$ has degree at most $2k - 2e - 2$.

Corollary 19 *Let k be an even integer and $r = 1$. If $\deg(\phi) < k$, then there exists a nonzero function g with degree at most 2 such that the product $g\tau$ has degree at most $\max\{2k - 4, k + \deg(\psi), k + \deg(\varphi)\}$.*

Proof. Taking $e = 1$ in the first half part of Theorem 18 gives this corollary. □

The above result shows that for even k and $r = 1$, if $\deg(\phi) < k$, $\deg(\psi) \leq k - 4$ and $\deg(\varphi) \leq k - 4$, then there exists a nonzero function g with degree at most 2 such that the product $g\tau$ has degree at most $2k - 4$.

5 The Immunity of the functions based on Carlet-Feng function against fast algebraic attacks

In recent years, several constructions of Boolean functions with maximum algebraic immunity and good nonlinearity are proposed based on bivariate polynomial representation and Carlet-Feng function ϕ_{CF}. The functions constructed by Z. Tu and Y. Deng [22] have the form $\phi_{CF}(xy^{2^k-2}) + (x^{2^k-1} + 1)\psi(y)$, the functions constructed by D. Tang et al. [21] have the form $\phi_{CF}(xy) + (x^{2^k-1} + 1)\psi(y)$, and the functions constructed by Q. Jin et al. [13] have the form $\phi_{CF}(xy^r) + (x^{2^k-1} + 1)\psi(y)$. Such functions have good

nonlinearity and might have maximum algebraic immunity (depending on whether a binary conjecture is correct[1]).

Some of these functions are observed through computer experiments to have good behavior against fast algebraic attacks, but no mathematical results are found in previous literatures. In this section, we further study these functions in terms of the immunity against fast algebraic attacks.

5.1 Carlet-Feng functions

Let α be a primitive element of $\mathbb{F}_{2^k}$. Let $\phi_{CF} \in \mathbf{B}_k$ and

$$\mathrm{supp}(\phi_{CF}) = \{\alpha^l, \alpha^{l+1}, \alpha^{l+2}, \cdots, \alpha^{l+2^{k-1}-1}\}, 0 \le l \le 2^k - 2. \tag{24}$$

The function ϕ_{CF}, called Carlet-Feng function, was first presented in [10] and further studied by C. Carlet and K. Feng [4]. Carlet-Feng function was proved in [17] to be optimal against fast algebraic attacks among all the functions with degree less than n.

Proposition 20 *[4] Let $\sum_{i=0}^{2^k-1} \phi_i x^i (\phi_i \in \mathbb{F}_{2^k})$ be the univariate representation of the function ϕ_{CF}. Then $\phi_0 = 0$, $\phi_{2^k-1} = 0$, and for $1 \le i \le 2^k - 2$,*

$$\phi_i = \frac{\alpha^{-il}}{1 + \alpha^{-i/2}}.$$

Hence the algebraic degree of ϕ_{CF} is equal to $k - 1$.

The following result is useful in the proof of Proposition 22 which leads to the main results of this section.

Lemma 21 *[17] Let*

$$A = \left(\frac{b_i c_j}{1 + \beta_i \gamma_j}\right)_{m \times m}$$

be an $m \times m$ matrix with $b_i, c_j, \beta_i, \gamma_j \in \mathbb{F}_{2^k}^*$, $\beta_i \gamma_j \ne 1$, $1 \le i, j \le m$. If $\beta_i \ne \beta_j$ and $\gamma_i \ne \gamma_j$ for $i \ne j$, then $\det(A) \ne 0$.

Hereinafter we denote $\mathcal{A} \times \mathcal{U} = \{(a, u) | a \in \mathcal{A}, u \in \mathcal{U}\}$. A similar proof of [17, Proposition 12] applies to the following theorem.

Proposition 22 *Let $\sum_{i=0}^{2^k-1} \phi_i x^i (\phi_i \in \mathbb{F}_{2^k})$ be the univariate representation of the function ϕ_{CF}. Let $\mathcal{A} \subset \{1, 2, \cdots, 2^k - 1\}$ and $\mathcal{U} \subset \{0, 1, \cdots, 2^k - 2\}$. Let A be a $\#\mathcal{A} \times \#\mathcal{U}$ matrix and*

$$A = (\phi_{a-u})_{\substack{a \in \mathcal{A} \\ u \in \mathcal{U}}}$$

where $a - u$ is considered as $a -_k u$. If one of the following conditions holds:

1. *$\#\mathcal{A} = \#\mathcal{U} \equiv 0 (\mathrm{mod}\, 2)$, $\mathcal{A} = \{2^k - 1 - u | u \in \mathcal{U}\}$, $\mathcal{A} \cap \mathcal{U} = \emptyset$, $(2^k - 1, 0) \in \mathcal{A} \times \mathcal{U}$,*
2. *$\#\mathcal{A} \ge \#\mathcal{U} + \#(\mathcal{A} \cap \mathcal{U})$, $(2^k - 1, 0) \notin \mathcal{A} \times \mathcal{U}$,*

then the matrix A has full column rank.

Proof. Case 1 has been proven in [17, Proposition 12].

For Case 2, let $\mathcal{A}^*$ be an arbitrary subset of $\mathcal{A} \setminus \mathcal{U}$ such that $\#\mathcal{A}^* = \#\mathcal{U}$. Let A^* be the matrix formed by selecting rows $\mathcal{A}^*$ from A, that is,

$$A^* = (\phi_{a-u})_{\substack{a \in \mathcal{A}^* \\ u \in \mathcal{U}}}.$$

For $a \in \mathcal{A}^*$ and $u \in \mathcal{U}$, we have $1 \le a -_k u \le 2^k - 2$, and thus by Proposition 20,

$$\phi_{a-u} = \frac{\alpha^{-al} \alpha^{ul}}{1 + \alpha^{-a/2} \alpha^{u/2}}.$$

It is derived from Lemma 21 that $\det(A^*) \ne 0$. Hence the matrix A has full column rank. □

[1] The conjecture for D. Tang et al.'s functions was proven in [5].

5.2 Jin et al.'s functions

Now we study the immunity against fast algebraic attacks of the function

$$\tau_{CF}(x,y) = \phi_{CF}(xy^r) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x), \tag{25}$$

where ϕ_{CF} is the function defined by (24) and ψ and φ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$, $\deg(\psi) < k$, $\deg(\varphi) < k$. The functions of Q. Jin et al. [13] are contained in the family of τ_{CF}.

Lemma 23 *Let $1 \le e \le k-1 \le d \le 2k-e-1$ and $0 \le t \le 2^k-2$.*

1. *If $\#\mathcal{W}_{e,r,0}$ is even, then $B(\phi_{CF}(xy^r); e, d; r, 0)$ has full column rank.*
2. *If $\#\overline{\mathcal{W}}_{d,r,t} \ge \#\mathcal{W}_{e,r,t}$, $t \ne 0$ and $k+e \le d$, then $B(\phi_{CF}(xy^r); e, d; r, t)$ has full column rank.*
3. *If $\#\overline{\mathcal{W}}^*_{d,r,t} \ge \#\mathcal{W}_{e,r,t}$, then $B^*(\phi_{CF}(xy^r); e, d; r, t)$ has full column rank.*

Proof. 1) By Proposition 6 and Proposition 7, when $\#\mathcal{W}_{e,r,0}$ is even, the matrix $B(\phi_{CF}(xy^r); e, 2k-e-1; r, 0)$ falls into Case 1 of Proposition 22 and thus has full column rank. Therefore $B(\phi_{CF}(xy^r); e, d; r, 0)$ has full column rank for $d \le 2k-e-1$.

2) By Proposition 9, when $k+e \le d$ and $\#\overline{\mathcal{W}}_{d,r,t} \ge \#\mathcal{W}_{e,r,t}$, the matrix $B(\phi_{CF}(xy^r); e, d; r, t)$ with $t \ne 0$ falls into Case 2 of Proposition 22 and thus has full column rank.

3) By Proposition 10, when $\#\overline{\mathcal{W}}^*_{d,r,t} \ge \#\mathcal{W}_{e,r,t}$, the matrix $B^*(\phi_{CF}(xy^r); e, d; r, t)$ falls into Case 2 of Proposition 22 and thus has full column rank. □

Theorem 24 *Let $1 \le e \le k-1$ and $e+k \le d \le 2k-e-1$. If $\#\overline{\mathcal{W}}_{d,r,t} \ge \#\mathcal{W}_{e,r,t}$ for $1 \le t \le 2^k-2$ and one of the following two conditions is satisfied:*

1. *$\#\mathcal{W}_{e,r,0}$ is even,*
2. *$\#\overline{\mathcal{W}}^*_{d,r,0} \ge \#\mathcal{W}_{e,r,0}$,*

then there exists no nonzero function $g \in \mathbf{B}_{2k}$ with degree at most e such that the product $g(x,y)\phi_{CF}(xy^r)$ has degree at most d.

Proof. It is obtained by Theorem 11 and Lemma 23. □

Theorem 25 *Let $1 \le e \le k-1 \le d \le 2k-e-1$. If $\#\overline{\mathcal{W}}^*_{d,r,t} \ge \#\mathcal{W}_{e,r,t}$ for $1 \le t \le 2^k-2$ and one of the following two conditions is satisfied:*

1. *$\#\mathcal{W}_{e,r,0}$ is even,*
2. *$\#\overline{\mathcal{W}}^*_{d,r,0} \ge \#\mathcal{W}_{e,r,0}$,*

then there exists no nonzero function $g \in \mathbf{B}_{2k}$ with degree at most e such that the product $g\tau_{CF}$ has degree at most d.

Proof. It is obtained by Corollary 16 and Corollary 17 and Lemma 23. □

Based on the above results, we propose an extremely efficient algorithm to determine the immunity of the function τ_{CF} described in (25) against fast algebraic attacks, see Algorithm 2 of Appendix E.

5.3 Tang et al.'s functions

In this section, we study the immunity against fast algebraic attacks of the function

$$\tau_{CF}(x,y) = \phi_{CF}(xy) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x), \tag{26}$$

where ϕ_{CF} is the function defined by (24) and ψ and φ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$, $\deg(\psi) < k$, $\deg(\varphi) < k$. The functions of D. Tang et al. [13] are contained in the family of the functions described in (26).

It was observed through computer experiments that some of D. Tang et al.'s functions have good behavior against fast algebraic attacks. Theorem 18 and Corollary 19 have shown the upper bounds on the immunity of these functions against fast algebraic attacks, while the following results show their lower bounds.

Theorem 26 *Let $k \geq 3$, $r = 1$ and $1 \leq e < k$. If e is even and $\binom{k-1}{\frac{e}{2}} \equiv 1 (\mathrm{mod}\, 2)$, the $2k$-variable function τ_{CF} admits no nonzero function $g \in \mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau_{CF}$ has degree at most $2k-e-3$; otherwise, the function τ_{CF} admits no nonzero function $g \in \mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau_{CF}$ has degree at most $2k-e-2$.*

Proof. By Lemma 32 and Lemma 33, it holds for $0 \leq t \leq 2^k - 2$ that $\#\overline{\mathcal{W}}^*_{2k-e-3,1,t} \geq \#\mathcal{W}_{e,1,t}$ when e is even, and the first half part of the theorem is derived by Theorem 25.

By Lemma 32, we have $\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \geq \#\mathcal{W}_{e,1,t}$ for $1 \leq t \leq 2^k - 2$. By Lemma 33 we have $\#\overline{\mathcal{W}}^*_{2k-e-2,1,0} \geq \#\mathcal{W}_{e,1,0}$ when e is odd. The same proof of Lemma 33 shows that $\#\overline{\mathcal{W}}_{e,1,0} = \sum_{i=0}^{\frac{e}{2}} \binom{k}{i}$ when e is even. Since $\sum_{i=0}^{\frac{e}{2}} \binom{k}{i} \equiv \binom{k-1}{\frac{e}{2}} (\mathrm{mod}\, 2)$, $\#\overline{\mathcal{W}}_{e,1,0}$ is even when $\binom{k-1}{\frac{e}{2}} \equiv 0 (\mathrm{mod}\, 2)$. Hence the second half part of the theorem is obtained by Theorem 25. □

For the case that e is even and $\binom{k-1}{\frac{e}{2}} \equiv 1 (\mathrm{mod}\, 2)$, there is only one nonzero function g with degree at most e such that $g\tau_{CF}$ has degree at most $2k-e-3$, where the function g has the form of $g^*(xy)$ with $g^* \in \mathbf{B}_k$ and $g^*(0) = 1$.

Corollary 27 *Let $k \geq 3$ and $r = 1$. Then $\mathcal{AI}(\tau_{CF}) = k$.*

Proof. If k is odd, then $\binom{k-1}{\frac{k-1}{2}} = 2\binom{k-2}{\frac{k-3}{2}} \equiv 0 (\mathrm{mod}\, 2)$; if k is even, then $k-1$ is odd. Taking $e = k-1$ in Theorem 26 gives this corollary. □

In [21], two special cases of Corollary 27 was proved: the function $\phi_{CF}(xy)$ and the function $\phi_{CF}(xy) + (x^{2^k-1}+1)\psi(y)$ with $\deg(\psi) = k-1$ have maximum $\mathcal{AI}$.

Theorem 28 *Let $k \geq 3$ and $r = 1$. If the univariate polynomial representation of ψ or φ has a monomial with algebraic degree equal to $k-1$, $k-2$ (when $k \geq 4$), or $k-3$ (when $k \geq 6$), then for any positive integer e with $e < k$, the $2k$-variable function τ_{CF} admits no nonzero function $g \in \mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau_{CF}$ has degree at most $2k-e-2$.*

Proof. By Theorem 26 it is sufficient to prove the theorem for $e \geq 2$. Let $d = 2k-e-2$. Lemma 32 states that $\#\overline{\mathcal{W}}^*_{d,1,t} \geq \#\mathcal{W}_{e,1,t}$ for $1 \leq t \leq 2^k - 2$. By Lemma 23, $B^*(\phi_{CF}(xy); e, d; 1, t)$ has full column rank for $1 \leq t \leq 2^k - 2$. Then from Theorem 15 we just need to prove the matrix $B^+(\tau_{CF}; e, d; 1, 0)$ has full column rank.

Assume that the univariate polynomial representation of ψ has a monomial y^b with algebraic degree equal to $k-1$, that is, $\mathrm{wt}(b) = k-1$. Let $\psi_b \neq 0$ be the coefficient of y^b in the univariate polynomial representation of ψ, let $\sum_{i=0}^{2^k-1} \phi_i x^i$, $\phi_i \in \mathbb{F}_{2^k}$, be the univariate polynomial representation of ϕ_{CF}, and let $\sum_{i=0}^{2^k-1}\sum_{i=0}^{2^k-1} \tau_{ij} x^i y^j$, $\tau_{ij} \in \mathbb{F}_{2^k}$, be the bivariate polynomial representation of $\tau_{CF}(x, y)$. Since $\phi_{CF}(xy) = \sum_{i=0}^{2^k-1} \phi_i x^i y^i$ and

$$\tau_{CF}(x, y) = \phi_{CF}(xy) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x),$$

we have $\tau_{2^k-1,b} = \psi_b$ and $\tau_{2^k-1-j,b-j} = 0$ for $1 \leq j \leq 2^k - 2$ and $j \neq b$ (since $2^k - 1 - j \neq b -_k j$, $2^k - 1 - j \notin \{2^k - 1, 0\}$ and $b -_k j \notin \{2^k - 1, 0\}$). By (15) we have $\mathcal{W}_{e,1,0} = \{(u, u) | \mathrm{wt}(u) \leq \frac{e}{2}\}$.

Thus for $(u,v) \in \mathcal{W}_{e,1,0}$, where $e < k$, we know $u = v$ and $\mathrm{wt}(v) < k/2 \le k-1 = \mathrm{wt}(b)$, where $k \ge 3$, and thus $u = v \ne 2^k - 1$ and $u = v \ne b$. Therefore, for $(u,v) \in \mathcal{W}_{e,1,0}$, it follows from (9) that $\lambda^{\tau_{CF}}_{(2^k-1,b),(u,v)} = \tau_{2^k-1-u,b-u}$ and thus, as mentioned above,

$$\lambda^{\tau_{CF}}_{(2^k-1,b),(u,v)} = \begin{cases} \psi_b, & \text{if } (u,v) = (0,0), \\ 0, & \text{otherwise.} \end{cases}$$

Since $\mathrm{wt}(b) = k-1$, we know $(2^k-1,b) \in \overline{\mathcal{W}}_{2k-2} \subset \overline{\mathcal{W}}_d$ and thus $(2^k-1,b) \in \overline{\mathcal{W}}^+_{d,1,0}$, for $d = 2k-e-2$ with $e \ge 2$. Since $\psi_b \ne 0$, from the definition of $B^+(f;e,d;1,0)$ it is sufficient to prove the matrix

$$B^*_*(f;e,d;1,0) = \left(\lambda^{\tau_{CF}}_{(a,b),(u,v)}\right)_{\substack{(a,b)\in\overline{\mathcal{W}}^*_{d,1,0} \\ (u,v)\in\mathcal{W}^*_{e,1,0}}}$$

has full column rank. By Lemma 29 we have $\#\overline{\mathcal{W}}_{2k-e-1,1,0} = \#\mathcal{W}_{e,1,0}$ and thus $\#\overline{\mathcal{W}}^*_{d,1,0} \ge \#\overline{\mathcal{W}}^*_{2k-e-1,1,0} = \#\mathcal{W}^*_{e,1,0}$. The same proof of Lemma 23 shows that $B^*_*(f;e,d;1,0)$ has full column rank. Hence we have proven that the matrix $B^+(\tau_{CF};e,d;1,0)$ has full column rank.

For the case $\mathrm{wt}(b) = k-2$ with $k \ge 4$ or $\mathrm{wt}(b) = k-3$ with $k \ge 6$, we have $\mathrm{wt}(b) \ge k/2$ and $(2^k-1,b) \in \overline{\mathcal{W}}^+_{d,1,0}$ for $d = 2k-e-2$ with $e \ge 2$, and thus we can obtain the result using the same proof method.

The same proof shows that the theorem is true when the univariate polynomial representation of φ has a monomial with algebraic degree equal to $k-1$, $k-2$ (when $k \ge 4$), or $k-3$ (when $k \ge 6$). □

Theorem 26 and Theorem 28 state that the function

$$\phi_{CF}(xy) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x)$$

achieves (almost) optimal immunity against fast algebraic attacks.

The same proof of Theorem 28 shows that for $k = 2^m t + 1$ with $t > 1$ odd, if $k - 2^m - 1 \le \max\{\deg(\psi), \deg(\varphi)\} \le k-1$, then for any positive integer e with $e < k$, the $2k$-variable function τ_{CF} admits no nonzero function $g \in \mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau_{CF}$ has degree at most $2k-e-2$.

6 Conclusion

In this paper, we assess the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation by checking whether the matrix $B(f;e,d)$ has full column rank. In particular, we establish a method for efficiently evaluating the immunity against fast algebraic attacks of the family of $2k$-variable Boolean functions

$$\tau(x,y) = \phi(xy^r) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x).$$

For these functions, submatrices of $B(f;e,d)$ are used to estimate the immunity against fast algebraic attacks. When ϕ is a Carlet-Feng function, the estimation becomes more efficient: we only need to compare cardinalities of $(2^k-1)/k$ pairs of sets. Based on the results comparing cardinalities of such sets for $r = 1$, we prove that the functions of D. Tang et al. are (almost) optimal against fast algebraic attacks.

Acknowledgement

Meicheng Liu would like to thank Tianze Wang for his helpful discussions on bivariate polynomial representation of Boolean functions and careful checking of the results of Appendix C of this manuscript.

References

1. F. Armknecht. Improving fast algebraic attacks. In: B. Roy and W. Meier (eds.) FSE 2004. LNCS vol. 3017, pp. 65–82. Berlin, Heidelberg: Springer, 2004.
2. F. Armknecht, C. Carlet, P. Gaborit, et al. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In: S. Vaudenay (eds.) EUROCRYPT 2006. LNCS vol. 4004, pp. 147–164. Berlin, Heidelberg: Springer, 2006.
3. C. Carlet. Boolean functions for cryptography and error correcting codes. In: Y. Crama, P. Hammer, eds. Boolean Methods and Models in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge: Cambridge University Press, 2010.
4. C. Carlet and K. Feng. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: ASIACRYPT 2008, LNCS vol. 5350, 425–440. Berlin, Heidelberg: Springer, 2008.
5. G. Cohen and J. P. Flori. On a generalized combinatorial conjecture involving addition mod $2^k - 1$. Cryptology ePrint Archive, Report 2011/400, http://eprint.iacr.org/
6. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-EUROCRYPT 2003, LNCS 2656, 345–359. Berlin, Heidelberg: Springer, 2003.
7. N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-CRYPTO 2003, LNCS 2729, 176–194. Berlin, Heidelberg: Springer, 2003.
8. N. Courtois. Cryptanalysis of Sfinks. ICISC 2005, Lecture Notes in Computer Science, Volume 3935, 261–269. Berlin, Heidelberg: Springer, 2006.
9. D. K. Dalai, S. Maitra, and S. Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Designs, Codes and Cryptography, vol. 40, no. 1, 41–58, 2006.
10. K. Feng, Q. Liao, and J. Yang. Maximal values of generalized algebraic immunity. Designs, Codes and Cryptography, vol. 50, no. 2, pp. 243–252, 2009.
11. S. Fischer and W. Meier. Algebraic immunity of S-boxes and augmented functions. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 366–381. Springer, 2007.
12. P. Hawkes and G. Rose. Rewriting variables: the complexity of fast algebraic attacks on stream ciphers, in Crypto 2004, LNCS 3152, pp. 390–406. Springer, 2004.
13. Q. Jin, Z. Liu, B. Wu, et al. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity. Cryptology ePrint Archive, Report 2011/515, http://eprint.iacr.org/
14. N. Li, L. Qu, W. Qi, et al. On the construction of Boolean Functions with optimal algebraic immunity. IEEE Transactions on Information Theory, vol. 54, no. 3, 1330–1334, 2008.
15. N. Li and W. Qi. Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity. ASIACRYPT 2006, LNCS 4284, pp. 84–98. Berlin, Heidelberg: Springer, 2006.
16. M. Liu, D. Lin, and D. Pei. Fast algebraic attacks and decomposition of symmetric Boolean functions. IEEE Transactions on Information Theory, vol. 57, no. 7, pp. 4817–4821, 2011.
17. M. Liu, Y. Zhang, and D. Lin. Perfect algebraic immune functions. ASIACRYPT 2012. To appear in LNCS, Springer 2012. An extended version is available at `http://eprint.iacr.org/2012/212/`.
18. W. Meier, E. Pasalic, and C. Carlet. Algebraic attacks and decomposition of Boolean functions. Advances in Cryptology-EUROCRYPT 2004, LNCS 3027, 474–491. Berlin, Heidelberg: Springer, 2004.
19. P. Rizomiliotis. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation. IEEE Transactions on Information Theory, vol. 56, no. 8, pp. 4014–4024, 2010.
20. P. Rizomiliotis. On the security of the Feng-Liao-Yang Boolean functions with optimal algebraic immunity against fast algebraic attacks. Designs, Codes and Cryptography, vol. 57, no. 3, pp. 283-292, 2010.
21. D. Tang, C. Carlet, and X. Tang. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. Cryptology ePrint Archive, Report 2011/366, http://eprint.iacr.org/
22. Z. Tu and Y. Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Designs, Codes and Cryptography, vol. 60, no. 1, pp. 1–14, 2011.
23. X. Zeng, C. Carlet, J. Shan, and L. Hu. More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks. IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 6310–6320, 2011.
24. Y. Zhang, M. Liu, and D. Lin. On the immunity of rotation symmetric Boolean functions against fast algebraic attacks. Cryptology ePrint Archive, Report 2012/111, http://eprint.iacr.org/

A Example of bivariate polynomial representation

Example 1 *Let $n = 5$, $n_1 = 2$, $n_2 = 3$. A 5-variable Boolean function f considered as a mapping from $\mathbb{F}_{2^2} \times \mathbb{F}_{2^3}$ into $\mathbb{F}_2$ can be uniquely represented as*

$$f(x, y) = a_{00} + a_{01}y + a_{01}^2 y^2 + a_{01}^4 y^4 + a_{03}y^3 + a_{03}^2 y^6 + a_{03}^4 y^5 + a_{07}y^7$$

$$
\begin{aligned}
&+ a_{10}x + a_{10}^2x^2 + a_{11}xy + a_{11}^2x^2y^2 + a_{11}^4xy^4 + a_{11}^8x^2y + a_{11}^{16}xy^2 + a_{11}^{32}x^2y^4\\
&+ a_{13}xy^3 + a_{13}^2x^2y^6 + a_{13}^4xy^5 + a_{13}^8x^2y^3 + a_{13}^{16}xy^6 + a_{13}^{32}x^2y^5 + a_{17}xy^7 + a_{27}^2x^2y^7\\
&+ a_{30}x^3 + a_{31}x^3y + a_{31}^2x^3y^2 + a_{31}^4x^3y^4 + a_{33}x^3y^3 + a_{33}^2x^3y^6 + a_{33}^4x^3y^5 + a_{37}x^3y^7,
\end{aligned}
$$

where $a_{00}, a_{07}, a_{30}, a_{37} \in \mathbb{F}_2$, $a_{10}, a_{17} \in \mathbb{F}_{2^2}$, $a_{01}, a_{03}, a_{31}, a_{33} \in \mathbb{F}_{2^3}$ *and* $a_{11}, a_{13} \in \mathbb{F}_{2^6}$. *The number of such polynomials is exactly* $2^4 \cdot (2^2)^2 \cdot (2^3)^4 \cdot (2^6)^2 = 2^{2^5}$.

B Example of matrix $B(f; e, d)$

Example 2 *Let* $n = 5$, $n_1 = 2$, $n_2 = 3$, $e = 1$, $d = 3$. *Then*

$$\mathcal{W}_e = \{(0,0), (0,1), (0,2), (0,4), (1,0), (2,0)\}$$

and

$$\overline{\mathcal{W}}_d = \{(3,7), (3,6), (3,5), (3,3), (2,7), (1,7)\}.$$

Let $f(x,y) = \sum_{i=0}^{3}\sum_{j=0}^{7} f_{ij}x^iy^j$ *and* $g(x,y) = g_{00} + g_{01}y + g_{02}y^2 + g_{04}y^4 + g_{10}x + g_{20}x^2$, $f_{ij}, g_{ij} \in \mathbb{F}_{2^6}$. *Then*

$$
\begin{aligned}
h(x,y) =& g(x,y)f(x,y)\\
=& (g_{00} + g_{01}y + g_{02}y^2 + g_{04}y^4 + g_{10}x + g_{20}x^2)\sum_{i=0}^{3}\sum_{j=0}^{7} f_{ij}x^iy^j\\
=& (g_{00} + g_{01}y + g_{02}y^2 + g_{04}y^4 + g_{10}x + g_{20}x^2)f_{00}\\
&+ \sum_{i=1}^{3}(g_{00}f_{i0} + g_{01}f_{i7}y + g_{02}f_{i7}y^2 + g_{04}f_{i7}y^4 + g_{10}f_{i-1,0} + g_{20}f_{i-2,0})x^i\\
&+ \sum_{j=1}^{7}(g_{00}f_{0j} + g_{01}f_{0,j-1} + g_{02}f_{0,j-2} + g_{04}f_{0,j-4} + g_{10}f_{3j}x + g_{20}f_{3j}x^2)y^j\\
&+ \sum_{i=1}^{3}\sum_{j=1}^{7}(g_{00}f_{ij} + g_{01}f_{i,j-1} + g_{02}f_{i,j-2} + g_{04}f_{i,j-4} + g_{10}f_{i-1,j} + g_{20}f_{i-2,j})x^iy^j.
\end{aligned}
$$

We can see that

$$
\begin{aligned}
h_{37} =& g_{00}f_{37} + g_{01}f_{36} + g_{02}f_{35} + g_{04}f_{33} + g_{10}f_{27} + g_{20}f_{17},\\
h_{36} =& g_{00}f_{36} + g_{01}f_{35} + g_{02}f_{34} + g_{04}f_{32} + g_{10}f_{26} + g_{20}f_{16},\\
h_{35} =& g_{00}f_{35} + g_{01}f_{34} + g_{02}f_{33} + g_{04}f_{31} + g_{10}f_{25} + g_{20}f_{15},\\
h_{33} =& g_{00}f_{33} + g_{01}f_{32} + g_{02}f_{31} + g_{04}f_{36} + g_{10}f_{23} + g_{20}f_{13},\\
h_{27} =& g_{00}f_{27} + g_{01}f_{26} + g_{02}f_{25} + g_{04}f_{23} + g_{10}f_{17} + g_{20}(f_{07} + f_{37}),\\
h_{17} =& g_{00}f_{17} + g_{01}f_{16} + g_{02}f_{15} + g_{04}f_{13} + g_{10}(f_{07} + f_{37}) + g_{20}f_{27},
\end{aligned}
$$

and thus

$$
B(f;1,3) = \begin{pmatrix}
f_{37} & f_{36} & f_{35} & f_{33} & f_{27} & f_{17}\\
f_{36} & f_{35} & f_{34} & f_{32} & f_{26} & f_{16}\\
f_{35} & f_{34} & f_{33} & f_{31} & f_{25} & f_{15}\\
f_{33} & f_{32} & f_{31} & f_{36} & f_{23} & f_{13}\\
f_{27} & f_{26} & f_{25} & f_{23} & f_{17} & f_{07} + f_{37}\\
f_{17} & f_{16} & f_{15} & f_{13} & f_{07} + f_{37} & f_{27}
\end{pmatrix}.
$$

C Lemmas for proving Theorem 26 and Theorem 28

Lemma 29, Lemma 30 and Lemma 31 are used to prove Lemma 32 and Lemma 33. Lemma 32 and Lemma 33 are used to prove Theorem 26 and Theorem 28.

Lemma 29 *$\#\overline{\mathcal{W}}_{2k-e-1,1,t} = \#\mathcal{W}_{e,1,t}$ for $0 \le t \le 2^k-2$.*

Proof. Since $(a,b) \in \overline{\mathcal{W}}_{2k-e-1,1,t}$ if and only if $\mathrm{wt}(a)+\mathrm{wt}(b) \ge 2k-e$ and $b-a \equiv t \pmod{2^k-1}$, that is, $\mathrm{wt}(2^k-1-a)+\mathrm{wt}(2^k-1-b) \le e$ and $(2^k-1-a)-(2^k-1-b) \equiv t \pmod{2^k-1}$, it follows that $(a,b) \in \overline{\mathcal{W}}_{2k-e-1,1,t}$ if and only if $(2^k-1-b, 2^k-1-a) \in \mathcal{W}_{e,1,t}$. Therefore $\#\overline{\mathcal{W}}_{2k-e-1,1,t} = \#\mathcal{W}_{e,1,t}$. □

Remark 4. In [5], G. Cohen and J. P. Flori proved $\#\mathcal{W}_{k-1,1,t} \le 2^{k-1}$ for $1 \le t \le 2^k-2$. The same approach of [5] applies to Lemma 29.

Lemma 30 *Let $k \le d \le 2k-1$, $d-k+1 \le \mathrm{wt}(t)$ and $1 \le t \le 2^k-2$. If $\mathrm{wt}(t) \ge d-k+2$, then $\#\overline{\mathcal{W}}^*_{d-1,1,t} - \#\overline{\mathcal{W}}^*_{d,1,t} \ge 2$; if $\mathrm{wt}(t) = d-k+1$, then $\#\overline{\mathcal{W}}^*_{d-1,1,t} - \#\overline{\mathcal{W}}^*_{d,1,t} \ge 1$.*

Proof. If $\mathrm{wt}(t)+k-d$ is even, then there are $\binom{\mathrm{wt}(t)}{(\mathrm{wt}(t)+k-d)/2}$ pairs of integers (t_a,t_b) such that $t_a+t_b=t$, $\mathrm{supp}(t_a) \subset \mathrm{supp}(t)$, $\mathrm{supp}(t_b) \subset \mathrm{supp}(t)$, $\mathrm{wt}(t_a) = (\mathrm{wt}(t)+k-d)/2$ and $\mathrm{wt}(t_b) = (\mathrm{wt}(t)+d-k)/2$. Let $(a,b) = (2^k-1-t_a, t_b)$. Since $\mathrm{wt}(t) \ge d-k+1 \ge 1$, we know $\mathrm{wt}(t_a) \ne 0$ and $a \ne 2^k-1$; since $\mathrm{wt}(b) = \mathrm{wt}(t_b) < k$, we have $b \ne 2^k-1$. Then $(a,b) \notin \{(2^k-1,t),(2^k-1-t,2^k-1)\}$. Since $b-a \equiv t_a+t_b = t \pmod{2^k-1}$ and $\mathrm{wt}(a)+\mathrm{wt}(b) = k-\mathrm{wt}(t_a)+\mathrm{wt}(t_b) = k-(\mathrm{wt}(t)+k-d)/2+(\mathrm{wt}(t)+d-k)/2 = d$, we know $(a,b) \in \overline{\mathcal{W}}^*_{d-1,1,t} \setminus \overline{\mathcal{W}}^*_{d,1,t}$ and therefore $\#\overline{\mathcal{W}}^*_{d-1,1,t} - \#\overline{\mathcal{W}}^*_{d,1,t} \ge \binom{\mathrm{wt}(t)}{(\mathrm{wt}(t)+k-d)/2} \ge 2$ when $\mathrm{wt}(t) \ge d-k+2$.

If $\mathrm{wt}(t)+k-d$ is odd, then $\mathrm{wt}(t)+k-d-1$ is even and thus there are at least $\binom{\mathrm{wt}(t)-1}{(\mathrm{wt}(t)+k-d-1)/2}$ pairs of nonnegative integers (t_a,t_b) such that $t_a+t_b=t$, $\mathrm{supp}(t_a) \subset \mathrm{supp}(t)$, $\mathrm{supp}(t_b) \subset \mathrm{supp}(t)$, $\mathrm{wt}(t_a) = (\mathrm{wt}(t)+k-d-1)/2$, $\mathrm{wt}(t_b) = (\mathrm{wt}(t)+d+1-k)/2$ and $s+1 \in \mathrm{supp}(t_b)$, where s satisfies that $(s+1) \bmod k \in \mathrm{supp}(t)$ and $s \notin \mathrm{supp}(t)$ (since $t \ne 2^k-1$ we can always find such s). Let $(a,b) = (2^k-1-t_a-2^s, t_b-2^s)$. Since $\mathrm{supp}(t_b) \subset \mathrm{supp}(t)$, we know $s \notin \mathrm{supp}(t_a)$ and $s \notin \mathrm{supp}(t_b)$, and therefore $\mathrm{wt}(t_a+2^s) = \mathrm{wt}(t_a)+1$ and $\mathrm{wt}(t_b-2^s) = \mathrm{wt}(t_b)$ (noting that $s+1 \in \mathrm{supp}(t_b)$), which also shows that $a \ne 2^k-1$ and $b \ne 2^k-1$ and then $(a,b) \notin \{(2^k-1,t),(2^k-1-t,2^k-1)\}$. Since $b-a \equiv t_a+t_b = t \pmod{2^k-1}$ and $\mathrm{wt}(a)+\mathrm{wt}(b) = k-\mathrm{wt}(t_a+2^s)+\mathrm{wt}(t_b-2^s) = k-\mathrm{wt}(t_a)-1+\mathrm{wt}(t_b) = d$, we know $(a,b) \in \overline{\mathcal{W}}^*_{d-1,1,t} \setminus \overline{\mathcal{W}}^*_{d,1,t}$ and then $\#\overline{\mathcal{W}}^*_{d-1,1,t} - \#\overline{\mathcal{W}}^*_{d,1,t} \ge \binom{\mathrm{wt}(t)-1}{(\mathrm{wt}(t)+k-d-1)/2}$, which is greater than or equal to 2 when $\mathrm{wt}(t) \ge d-k+3$ and equal to 1 when $\mathrm{wt}(t) = d-k+1$. □

Lemma 31 *Let $k \le d \le 2k-1$, $\mathrm{wt}(t) \le 2k-d-1$ and $1 \le t \le 2^k-2$. If $\mathrm{wt}(t) \le 2k-d-2$, then $\#\overline{\mathcal{W}}^*_{d-1,1,t} - \#\overline{\mathcal{W}}^*_{d,1,t} \ge 2$; if $\mathrm{wt}(t) = 2k-d-1$, then $\#\overline{\mathcal{W}}^*_{d-1,1,t} - \#\overline{\mathcal{W}}^*_{d,1,t} \ge 1$.*

Proof. Since $(a,b) \in \overline{\mathcal{W}}_{d,1,t}$ if and only if $(b,a) \in \overline{\mathcal{W}}_{d,1,2^k-1-t}$, we have $\#\overline{\mathcal{W}}_{d,1,t} = \#\overline{\mathcal{W}}_{d,1,2^k-1-t}$, then the lemma is derived from Lemma 30 by replacing t with 2^k-1-t. □

Lemma 32 *Let $k \ge 3$, $1 \le e \le k-1$ and $1 \le t \le 2^k-2$. Then $\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \ge \#\mathcal{W}_{e,1,t}$.*

Proof. By Lemma 29 we know $\#\overline{\mathcal{W}}_{2k-e-1,1,t} = \#\mathcal{W}_{e,1,t}$, then taking $d = 2k-e-1$ in Lemma 30 gives $\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \ge \#\overline{\mathcal{W}}^*_{2k-e-1,1,t} + 2 \ge \#\mathcal{W}_{e,1,t}$ for $\mathrm{wt}(t) \ge k-e+1$; similarly, Lemma 31 shows $\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \ge \#\mathcal{W}_{e,1,t}$ for $\mathrm{wt}(t) \le e-1$. Therefore we just need to prove the lemma for $e \le wt(t) \le k-e$ with $e \le k/2$.

Denote $v_t = (2^k-1,t)$, $v_{-t} = (2^k-1-t, 2^k-1)$ and $\mathrm{wt}((a,b)) = \mathrm{wt}(a)+\mathrm{wt}(b)$. Then $\mathrm{wt}(v_t) = k+\mathrm{wt}(t)$ and $\mathrm{wt}(v_{-t}) = 2k-\mathrm{wt}(t)$.

For $e < k/2$, if $e < wt(t) < k-e$, then $\mathrm{wt}(v_t) < 2k-e$ and $\mathrm{wt}(v_{-t}) < 2k-e$, and thus $v_t \notin \overline{\mathcal{W}}_{2k-e-1,1,t}$ and $v_{-t} \notin \overline{\mathcal{W}}_{2k-e-1,1,t}$, showing that $\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \ge \#\overline{\mathcal{W}}^*_{2k-e-1,1,t} = \#\overline{\mathcal{W}}_{2k-e-1,1,t} = \#\mathcal{W}_{e,1,t}$; if $wt(t) = e$, then $\mathrm{wt}(v_t) = k+e < 2k-e$ and thus $v_t \notin \overline{\mathcal{W}}_{2k-e-1,1,t}$, and taking $d = 2k-e-1$ in Lemma 31 gives

$\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \geq \#\overline{\mathcal{W}}^*_{2k-e-1,1,t} + 1 \geq \#(\overline{\mathcal{W}}_{2k-e-1,1,t} \setminus \{v_t\}) = \#\overline{\mathcal{W}}_{2k-e-1,1,t} = \#\mathcal{W}_{e,1,t}$; if $wt(t) = k - e$, then $\mathrm{wt}(v_{-t}) = k + e < 2k - e$ and thus $v_{-t} \notin \overline{\mathcal{W}}_{2k-e-1,1,t}$, and taking $d = 2k - e - 1$ in Lemma 30 gives $\#\overline{\mathcal{W}}^*_{2k-e-2,1,t} \geq \#\overline{\mathcal{W}}^*_{2k-e-1,1,t} + 1 \geq \#(\overline{\mathcal{W}}_{2k-e-1,1,t} \setminus \{v_{-t}\}) = \#\overline{\mathcal{W}}_{2k-e-1,1,t} = \#\mathcal{W}_{e,1,t}$.

For $e = k/2$ and $e \leq \mathrm{wt}(t) \leq k - e$ with k even, we have $\mathrm{wt}(t) = k/2$. Then there is s with $0 \leq s \leq k - 1$ such that $\mathrm{wt}(t - 2^s) = \mathrm{wt}(t) = k/2$ and there is s^* with $0 \leq s^* \leq k - 1$ such that $\mathrm{wt}(2^k - 1 - t - 2^{s^*}) = \mathrm{wt}(2^k - 1 - t) = k/2$. We can check for $k \geq 4$ that $2^k - 1 - 2^s \neq 2^k - 1 - t - 2^{s^*}$, $(2^k - 1 - 2^s, t - 2^s) \in \overline{\mathcal{W}}^*_{3k/2-2,1,t} \setminus \overline{\mathcal{W}}^*_{3k/2-1,1,t}$ and $(2^k - 1 - t - 2^{s^*}, 2^k - 1 - 2^{s^*}) \in \overline{\mathcal{W}}^*_{3k/2-2,1,t} \setminus \overline{\mathcal{W}}^*_{3k/2-1,1,t}$, and therefore $\overline{\mathcal{W}}^*_{3k/2-2,1,t} \geq \overline{\mathcal{W}}^*_{3k/2-1,1,t} + 2 \geq \overline{\mathcal{W}}_{3k/2-1,1,t} = \overline{\mathcal{W}}_{k/2,1,t}$. □

Lemma 33 *Let $k \geq 3$ and $1 \leq e \leq k - 1$.*

If e is odd, then $\#\overline{\mathcal{W}}^*_{2k-e-2,1,0} \geq \#\mathcal{W}_{e,1,0}$.

If e is even, then $\#\overline{\mathcal{W}}^*_{2k-e-3,1,0} \geq \#\mathcal{W}_{e,1,0}$.

Proof. If e is odd, then by (16) we know

$$\begin{aligned}
&\#(\overline{\mathcal{W}}^*_{2k-e-2,1,0} \setminus \mathcal{W}_{2k-e-1,1,0}) \\
=&\#\{(a,a) | 2\,\mathrm{wt}(a) = 2k - e - 1, 1 \leq a \leq 2^k - 2\} \\
=&\binom{k}{\frac{e+1}{2}} \geq 3.
\end{aligned}$$

and hence $\#\overline{\mathcal{W}}^*_{2k-e-2,1,0} \geq \mathcal{W}^*_{2k-e-1,1,0} + 3 \geq \mathcal{W}_{2k-e-1,1,0} = \mathcal{W}_{e,1,0}$.

If e is even, then by (16) we know

$$\begin{aligned}
&\#(\overline{\mathcal{W}}^*_{2k-e-3,1,0} \setminus \mathcal{W}_{2k-e-1,1,0}) \\
=&\#\{(a,a) | 2k - e - 2 \leq 2\,\mathrm{wt}(a) \leq 2k - e - 1, 1 \leq a \leq 2^k - 2\} \\
=&\#\{a | 2\,\mathrm{wt}(a) = 2k - e - 2, 1 \leq a \leq 2^k - 2\} \\
=&\binom{k}{\frac{e+2}{2}} \geq 3,
\end{aligned}$$

and hence $\#\overline{\mathcal{W}}^*_{2k-e-3,1,0} \geq \mathcal{W}^*_{2k-e-1,1,0} + 3 \geq \mathcal{W}_{2k-e-1,1,0} = \mathcal{W}_{e,1,0}$. □

D Efficient computation of the immunity of the function τ against fast algebraic attacks

We propose an efficient algorithm to determine the immunity of the function τ described in (11) against fast algebraic attacks, see Algorithm 1. The algorithm is based on Theorem 2, Theorem 13 and Corollary 17. The outputs d^*, d_*, g_* satisfy that: (1) there is no nonzero function g with algebraic degree at most e such that $\deg(g\tau) < d^*$; (2) there is nonzero function g with algebraic degree at most e such that $\deg(g\tau) \leq d_*$; (3) $\deg(g_*) \leq e$ and $\deg(g_*\tau) \leq d_*$. The first two statements are derived from Corollary 17 and Theorem 13 respectively. The proof of Theorem 2 shows that g_* is a nonzero Boolean function and satisfies the third statement.

The algorithm requires that $\gcd(r, 2^k - 1) = 1$, $1 \leq e \leq k - 1$, $\phi_{2^k-1} \in \mathbb{F}_2$ and $\phi_{2i \bmod (2^n-1)} = \phi_i^2$ for $1 \leq i \leq 2^n - 2$. We need to check this before running the algorithm.

The algorithm can be improved based on Corollary 16: when computing d^*, we can add $2^k - 1$ to the set $\mathcal{A}$ for $t = 0$. The improved algorithm could produce d^* greater than that of the original algorithm.

Data: k, r, e, ϕ_1, ϕ_2, $\cdots$, ϕ_{2^k-1}
Result: maximize d^* such that there is no nonzero g such that $\deg(g) \le e$ and $\deg(g\tau) < d^*$; minimize d_* and find nonzero g_* such that $\deg(g_*) \le e$ and $\deg(g_*\tau) \le d_*$

$T \leftarrow \{\min\{t, 2t, \cdots, 2^{k-1}t\}_{\bmod(2^k-1)} | 1 \le t \le 2^k - 2\}$, $d_* \leftarrow 2k - e$, $d^* \leftarrow 2k - e - 1$, $t_* \leftarrow -1$;
for $t \in \{0\} \cup T$ **do**
  $\mathcal{A} \leftarrow \{a|(a,b) \in \overline{\mathcal{W}}_{d_*,r,t}\}$, $\mathcal{U} \leftarrow \{u|(u,v) \in \mathcal{W}^*_{e,r,t}\}$;
  $M \leftarrow (\phi_{a-u})_{\substack{a\in\mathcal{A}\\ u\in\mathcal{U}}}$;
  while *M has not full column rank* **and** $d_* \ge e$ **do**
    $d_* \leftarrow d_* - 1$, $t_* \leftarrow t$;
    $\mathcal{A} \leftarrow \{a|(a,b) \in \overline{\mathcal{W}}_{d_*,r,t}\}$;
    $M \leftarrow (\phi_{a-u})_{\substack{a\in\mathcal{A}\\ u\in\mathcal{U}}}$;
  end
  $d^* \leftarrow \min\{d^*, d_*\}$;
  $\mathcal{A} \leftarrow \{a|(a,b) \in \overline{\mathcal{W}}^*_{d^*,r,t}\}$, $\mathcal{U} \leftarrow \{u|(u,v) \in \mathcal{W}_{e,r,t}\}$;
  $M \leftarrow (\phi_{a-u})_{\substack{a\in\mathcal{A}\\ u\in\mathcal{U}}}$;
  while *M has not full column rank* **and** $d^* \ge e$ **do**
    $d^* \leftarrow d^* - 1$;
    $\mathcal{A} \leftarrow \{a|(a,b) \in \overline{\mathcal{W}}^*_{d^*,r,t}\}$;
    $M \leftarrow (\phi_{a-u})_{\substack{a\in\mathcal{A}\\ u\in\mathcal{U}}}$;
  end
end
$d^* \leftarrow d^* + 1$, $d_* \leftarrow d_* + 1$;
$\mathcal{A} \leftarrow \{a|(a,b) \in \overline{\mathcal{W}}_{d_*,r,t_*}\}$, $\mathcal{U} \leftarrow \{u|(u,v) \in \mathcal{W}^*_{e,r,t_*}\}$;
$M \leftarrow (\phi_{a-u})_{\substack{a\in\mathcal{A}\\ u\in\mathcal{U}}}$;
find a nonzero solution to $M\overline{g}^{\mathrm{T}} = 0$ with $\overline{g} = (g_u)_{u\in\mathcal{U}}$;
$g_* \leftarrow \sum_{u\in\mathcal{U}} g_u x^u y^{ru+t_*}$, $\alpha \leftarrow$ a primitive element of $\mathbb{F}_{2^k}$;
while $\mathrm{Tr}(g_*) = 0$ **do**
  $g_* \leftarrow \alpha g_*$;
end
return d^*, d_*, g_*;

Algorithm 1: Determine the immunity of the function τ against fast algebraic attacks

Next we discuss the complexity of Algorithm 1. The complexity depends on the outputs d^* and d_*, and heavily depends on the distribution of the sizes of the matrix M, i.e., the cardinalities of $\overline{\mathcal{W}}_{d,r,t}$ and $\mathcal{W}_{e,r,t}$. The best case is that $d^* = d_* = 2k - e - \varepsilon \approx 2k - e$ and the distribution is uniform. Let $E = \sum_{i=0}^{e} \binom{2k}{i}$ and $D = \sum_{i=2k-e-\varepsilon}^{2k} \binom{2k}{i}$. The average size of these matrices is $D_{avg} \times E_{avg}$ with $E_{avg} = 2^{-k}E$ and $D_{avg} = 2^{-k}D$. Then Algorithm 1 takes $\mathcal{O}(D_{avg}E_{avg}) = \mathcal{O}(DE/2^{2k})$ memory. Determining whether M has not full column rank runs in $\mathcal{O}(D_{avg}E^2_{avg})$ operations, and solving the equations $M\overline{g}^{\mathrm{T}} = 0$ runs in $\mathcal{O}(D^2_{avg}E_{avg})$ operations. Time complexity of Algorithm 1 is $\mathcal{O}(\#T \cdot D_{avg}E^2_{avg} + D^2_{avg}E_{avg}) = \mathcal{O}((2^kE/k + D)DE/2^{3k})$. Compared to the space complexity $\mathcal{O}(E^2)$ and the time complexity $\mathcal{O}(DE^2)$ of Algorithm 2 in [2], Algorithm 1 is very efficient. Moveover, Algorithm 1 automatically searches for d and optimizes d, while the value of d of Algorithm 2 in [2] is given.

E Efficient computation of the immunity of the function τ_{CF} against fast algebraic attacks

In this section, we propose an extremely efficient algorithm to determine the immunity of the function τ_{CF} described in (25) against fast algebraic attacks, see Algorithm 2. The algorithm takes at most $\mathcal{O}(2^k)$ memory and runs in at most $\mathcal{O}(2^{2k}/k)$ operations.

Data: k, r, e
Result: maximize d^* such that there is no nonzero g such that $\deg(g) \le e$ and $\deg(g\tau_{CF}) < d^*$;
minimize d_* such that there is nonzero g such that $\deg(g) \le e$ and $\deg(g\tau_{CF}) \le d_*$

$T \leftarrow \{\min\{t, 2t, \cdots, 2^{k-1}t\}_{\bmod(2^k-1)} | 1 \le t \le 2^k - 2\}$;
if $\binom{2k-1}{e} \equiv 1 (\bmod 2)$ **then**
  $d \leftarrow 2k - e - 2$;
else
  $d \leftarrow 2k - e - 1$;
end
for $t \in T$ **do**
  while $\#\overline{\mathcal{W}}_{d,r,t} < \#\mathcal{W}^*_{e,r,t}$ **and** $d \ge k - 1$ **do**
    $d \leftarrow d - 1$;
  end
end
$d_* \leftarrow d + 1$;
for $t \in T$ **do**
  while $\#\overline{\mathcal{W}}^*_{d,r,t} < \#\mathcal{W}_{e,r,t}$ **and** $d \ge k - 1$ **do**
    $d \leftarrow d - 1$;
  end
end
while $\#\mathcal{W}_{e,r,0}$ *is odd* **and** $\#\overline{\mathcal{W}}^*_{d,r,0} < \#\mathcal{W}_{e,r,0}$ **and** $d \ge k - 1$ **do**
  $d \leftarrow d - 1$;
end
$d^* \leftarrow d + 1$;
return d^*, d_*;

Algorithm 2: Determine the immunity of the function τ_{CF} against fast algebraic attacks

The algorithm is an application of Theorem 1, Theorem 25 and Corollary 14. The outputs d^* and d_* satisfy that: (1) there is no nonzero function g with algebraic degree at most e such that $\deg(g\tau_{CF}) < d^*$; (2) there is nonzero function g with algebraic degree at most e such that $\deg(g\tau_{CF}) \le d_*$.

The second statement above is derived from Corollary 14, and thus also applies to the function τ. Then the output d_* of Algorithm 2 is more than or equal to the counterpart of Algorithm 1. This shows that if d_* is small, then the function τ described in (11), whatever the functions ϕ, ψ and φ are, is weak against against fast algebraic attacks.

As a matter of fact, Algorithm 2 searches for d^* and d_* through comparing the numbers of rows and columns of the matrices M in Algorithm 1. Then the output d^* of Algorithm 2 is also more than or equal to the counterpart of Algorithm 1. This shows that taking ϕ being a Carlet-Feng function to construct the function τ is an optimal choice in term of the immunity against fast algebraic attacks.

Note that $\#\overline{\mathcal{W}}_{d,r,t} = \#\overline{\mathcal{W}}_{d,2^s r^{-1},-2^s t}$ and $\#\mathcal{W}_{e,r,t} = \#\mathcal{W}_{e,2^s r^{-1},-2^s t}$. When we replace r with $2^s r^{-1}$ in Algorithm 2, it outputs the same results.

A similar algorithm also applies to the function τ with $\phi(x) = \phi_{CF}(x) + x^{2^k-1}$.

To conclude, we compare the algorithms proposed in this paper and Algorithm 2 in [2], see Table 1.

Table 1. Algorithms for computing the immunity against fast algebraic immunity

	Functions	Space Comp.	Time Comp.	d	output g
Alg.2 in [2]	all	E^2	DE^2	given	yes
Alg.1	τ	$DE/2^{2k}$	$(2^kE/k+D)DE/2^{3k}$	possible optimal	yes
Alg.2	τ_{CF}	2^k	$2^{2k}/k$	almost optimal	no

E.1 Experimental Results

Application of Algorithm 2 reveals that the probability that $\Delta d = 0$ is very high and almost all the cases satisfy $\Delta d \leq 1$, where $\Delta d = d_* - d^*$. The experimental results for $k = 5, 6, 7$ are listed in Table 2, 3, 4 respectively. Here, we only consider r such that $\gcd(r, 2^k - 1) = 1$ and $2 \leq \mathrm{wt}(r) \leq k - 2$, and $r, 2r, \cdots, 2^{k-1}r$ are considered as one case. Counting all the functions with $5 \leq k \leq 16$ and all e with $1 \leq e \leq k - 1$ gives $\Pr(\Delta d = 0) \approx 0.8$ and $\Pr(\Delta d \leq 1) \approx 0.9$. This result shows that Algorithm 2 and Theorem 25 are almost optimal for the function τ_{CF}. Moreover, it implies that the immunity of the function τ_{CF} against fast algebraic attacks appears to be less affected by the functions ψ and φ.

Also application of Algorithm 2 reveals that d^* is greater than or equal to k for any k and any r such that $5 \leq k \leq 16$, $\gcd(r, 2^k - 1) = 1$ and $1 \leq \mathrm{wt}(r) \leq k - 2$, e.g., see Table 2, 3, 4. Taking $e = k - 1$ gives $\mathcal{AI}(\tau_{CF}) = k$. Thus the function τ_{CF} described in (25) with $5 \leq k \leq 16$, whatever the functions ψ and φ are, has maximum $\mathcal{AI}$. Based on this observation, we propose a new conjecture as follows.

Conjecture 1. Let $k \geq 3$, $1 \leq r, t \leq 2^k - 2$, $\gcd(r, 2^k - 1) = 1$ and $1 \leq \mathrm{wt}(r) \leq k - 2$. Let

$$\mathcal{W}_{k-1,r,t} = \{(u, v) | \, \mathrm{wt}(u) + \mathrm{wt}(v) \leq k - 1, v \equiv ru + t (\mathrm{mod}\, 2^k - 1), 0 \leq u, v \leq 2^k - 2\}.$$

Then $\#\mathcal{W}_{k-1,r,t} \leq 2^{k-1} - 1$.

If the conjecture is correct, then the function τ_{CF} described in (25), whatever the functions ψ and φ are, has maximum $\mathcal{AI}$. The case $\mathrm{wt}(r) = 1$ has been proven in Section 5.3 (Corollary 27).

Further, application of Algorithm 2 reveals that for $5 \leq k \leq 16$ and $\gcd(r, 2^k - 1) = 1$: (1) $e + d^* \geq 2k - \min\{\mathrm{wt}(r), \mathrm{wt}(r^{-1})\}$ when $4 \leq \min\{\mathrm{wt}(r), \mathrm{wt}(r^{-1})\} \leq k-2$; (2) $e+d^* \geq 2k-\min\{\mathrm{wt}(r), \mathrm{wt}(r^{-1})\}-2$ when $\min\{\mathrm{wt}(r), \mathrm{wt}(r^{-1})\} = 2, 3$; (3) $e + d_* \leq 2k - 2$ for almost all r. The experimental results show that the behavior of the function τ_{CF} against fast algebraic attacks is not too bad, and that the functions τ_{CF} with $\mathrm{wt}(r) = 1$ have the best behavior against fast algebraic attacks among such functions.

Table 2. The immunity of 10-variable function τ_{CF} against fast algebraic immunity ($k = 5$)

r	3			5			7			11		
e	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd
1	7	8	1	7	8	1	7	8	1	7	8	1
2	7	8	1	7	8	1	7	8	1	7	8	1
3	6	6	0	6	7	1	6	7	1	6	6	0
4	5	6	1	5	6	1	5	6	1	5	6	1

Table 3. The immunity of 12-variable function τ_{CF} against fast algebraic immunity ($k = 6$)

r	5			11			13			23		
e	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd
1	9	10	1	8	10	2	9	10	1	8	10	2
2	8	9	1	8	9	1	8	9	1	8	9	1
3	8	8	0	8	8	0	8	8	0	8	8	0
4	7	7	0	7	7	0	7	7	0	7	7	0
5	6	6	0	6	6	0	6	6	0	6	6	0

Table 4. The immunity of 14-variable function τ_{CF} against fast algebraic immunity ($k = 7$)

r	3			5			7			9			11			13		
e	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd
1	11	12	1	11	12	1	10	12	2	11	12	1	10	12	2	10	12	2
2	11	11	0	11	11	0	10	11	1	10	11	1	10	12	2	10	12	2
3	10	10	0	10	10	0	10	10	0	10	10	0	10	10	0	10	10	0
4	9	9	0	9	9	0	9	9	0	9	9	0	9	9	0	9	9	0
5	8	8	0	8	8	0	8	8	0	8	8	0	8	8	0	8	8	0
6	7	8	1	7	7	0	7	7	0	7	7	0	7	7	0	7	7	0

r	15			19			21			23			27			29		
e	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd
1	11	12	1	10	12	2	10	12	2	10	12	2	11	12	1	10	12	2
2	10	11	1	10	11	1	10	11	1	10	11	1	11	11	0	10	11	1
3	10	10	0	10	10	0	10	10	0	10	10	0	10	10	0	10	10	0
4	9	9	0	9	9	0	9	9	0	9	9	0	9	9	0	9	9	0
5	8	8	0	8	8	0	8	8	0	8	8	0	8	8	0	8	8	0
6	7	7	0	7	7	0	7	7	0	7	8	1	7	7	0	7	8	1

r	31			43			47			55		
e	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd	d^*	d_*	Δd
1	10	12	2	11	12	1	10	12	2	10	12	2
2	10	11	1	11	11	0	10	11	1	10	11	1
3	10	10	0	10	10	0	10	10	0	10	10	0
4	9	9	0	9	9	0	9	9	0	9	9	0
5	8	8	0	8	8	0	8	8	0	8	8	0
6	7	7	0	7	8	1	7	7	0	7	7	0