Notion of Algebraic Immunity and Its evaluation Related to Fast Algebraic Attacks

Deepak Kumar Dalai[1], Kishan Chand Gupta[2]⋆ and Subhamoy Maitra[1]

[1] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 108, INDIA
{deepak_r, subho}@isical.ac.in

[2] Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1.
kgupta@math.uwaterloo.ca

Abstract. It has been noted recently that algebraic (annihilator) immunity alone does not provide sufficient resistance against algebraic attacks. In this regard, given a Boolean function f, just checking the minimum degree annihilators of $f, 1+f$ is not enough and one should check the relationships of the form $fg = h$, and a function f, even if it has very good algebraic immunity, is not necessarily good against fast algebraic attack, if degree of g becomes very low when degree of h is equal to or little greater than the algebraic immunity of f. In this paper we theoretically study the two currently known constructions having maximum possible algebraic immunity from this viewpoint. To the end, we also experimentally study some cryptographically significant functions having good algebraic immunity.

Keywords: Algebraic Attacks, Annihilators, Boolean Functions, Fast Algebraic Attacks.

1 Introduction

Algebraic attack and fast algebraic attack have recently received a lot of attention in cryptographic literature [3, 4, 15–19, 24, 27]. The study on algebraic attack identified an important property for Boolean functions to be used in crypto systems, which is called algebraic immunity [27, 21]. Using good algebraic immunity one may achieve resistance against algebraic attacks done in a particular way, i.e., using linearization. In fact, one may not need linearization if algorithms using Gröbner bases can be properly exploited. This is the reason in one of the recent papers [23], the term annihilator immunity is used instead of algebraic immunity. Further it should be noted that based on some recent works related to fast algebraic attacks [2, 19, 9, 1], one should concentrate more

⋆ This work has been done while the author has been visiting Indian Statistical Institute during December 2005–January 2006.

carefully on the design parameters of Boolean functions for proper resistance. The weakness of algebraic (annihilator) immunity against fast algebraic attack has been demonstrated in [20] by mounting an attack on SFINKS [8].

Let B_n be the set of all Boolean functions $\{0,1\}^n \rightarrow \{0,1\}$ on n input variables. One may refer to [21] for the definitions of truth table, algebraic normal form (ANF), algebraic degree (deg), weight (wt), nonlinearity (nl) and Walsh spectrum of a Boolean function.

The ANF of a Boolean function can be considered as a multivariate polynomial over GF(2). It is shown in [18] that, given any n-variable Boolean function f, it is always possible to get a Boolean function g with degree at most $\lceil \frac{n}{2} \rceil$ such that fg has degree at most $\lceil \frac{n}{2} \rceil$. Thus, while choosing a function f, the cryptosystem designer should be careful that it should not happen that the degree of fg falls much below $\lceil \frac{n}{2} \rceil$ with a nonzero function g whose degree is also much below $\lceil \frac{n}{2} \rceil$.

Definition 1. *Given $f \in B_n$, define $AN(f) = \{g \in B_n | \, f*g = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f.*

Note that we are mostly interested in the lowest degree nonzero annihilator.

Definition 2. *Given $f \in B_n$, its algebraic immunity is defined as [21] the minimum degree of all nonzero annihilators of f or $f + 1$, and it is denoted by $\mathcal{AI}_n(f)$.*

Note that $\mathcal{AI}_n(f) \leq \deg(f)$, since $f * (1 + f) = 0$. It can also be deduced from [18] that $\mathcal{AI}_n(f) \leq \lceil \frac{n}{2} \rceil$. Boolean functions and related results with algebraic (annihilator) immunity has currently received serious attention [5–7, 10, 11, 14, 12, 21–23, 27, 25] and the first two constructions of Boolean functions having maximum algebraic (annihilator) immunity is presented in [22, 23].

Now consider a function f with maximum possible algebraic immunity $\lceil \frac{n}{2} \rceil$. It may very well happen that in that case $fg = h$, where $\deg(h) = \lceil \frac{n}{2} \rceil$, but $\deg(g) < \lceil \frac{n}{2} \rceil$. In that case the lower degree of g may be exploited to mount a fast attack (well known as fast algebraic attack) even if the algebraic immunity of f is the maximum possible. In fact, there are examples, where one can get a linear g too. Initial study of Boolean functions in this area has been started in [9, 1]. Since algebraic immunity is now understood as a necessary (but not sufficient) condition against resisting algebraic and fast algebraic attacks, we feel there is a need to consider the functions with full algebraic immunity for their performance in terms of $fg = h$ relationship. That is for the functions f with full algebraic immunity we consider $\deg(h) \geq \lceil \frac{n}{2} \rceil$, and then after fixing the degree of h, we try to get the minimum degree g.

It is always meaningful to consider $fg = h$ only when $\deg(g) \leq \deg(h)$ as otherwise $fg = h$ will imply $fh = h$. So for all the discussion in this paper we will consider $\deg(g) \leq \deg(h)$ for a relation $fg = h$ unless mentioned otherwise.

In the next subsection we present a few preliminary technical results. In Section 2, we study the construction presented in [22]. In Section 3, we explore the symmetric and rotation symmetric functions. We also study the (modified) balanced Patterson-Wiedemann type functions in this direction [28, 29, 26].

1.1 Preliminary technical results

Proposition 1. *Consider an n-variable (n odd) function f having $\mathcal{AI}_n = \lceil \frac{n}{2} \rceil$. Then there will always exist g, h, such that $fg = h$, where $\deg(g) = \lfloor \frac{n}{2} \rfloor$ and $\deg(h) = \lceil \frac{n}{2} \rceil$.*

Proof. By [19, Theorem 7.2.1], we know that there always exists g, h, such that $fg = h$, with $\deg(g)+\deg(h) = n$. Thus, if we fix $\deg(g) = \lfloor \frac{n}{2} \rfloor$ and $\deg(h) = \lceil \frac{n}{2} \rceil$, we get the required result. □

Note that this always means that even if a function on odd number of variables n has full algebraic immunity $\lceil \frac{n}{2} \rceil$, one will always get a g one degree lower than that. However, for even n, this may or may not be true. In this paper we will show that given a Boolean function on n variables with full algebraic immunity $\frac{n}{2}$, one may or may not get a g having degree $< \frac{n}{2}$ such that $fg = h$ when $\deg(h) = \frac{n}{2}$.

Proposition 2. *Consider an n-variable function f. Consider the relationship $fg = h$, such that $\deg(h) = \mathcal{AI}_n(f)$. Then if degree of $g < \mathcal{AI}_n(f)$ then both $f, 1+f$ have minimum degree annihilators at degree $\mathcal{AI}_n(f)$.*

Proof. Consider the relations of the form $fg = h$, when $\deg(g) < \deg(h)$. From [9, Lemma 1], $fg = h$ iff $f(g+h) = 0$ & $(1+f)h = 0$. As $\deg(g) < \deg(h)$, we have $\deg(g+h) = \deg(h) = \mathcal{AI}_n(f)$. Thus both $f, 1+f$ have annihilators at degree $\mathcal{AI}_n(f)$. □

The following corollary is immediate from Proposition 2.

Corollary 1. *Let only one of $f, 1+f$ has minimum degree annihilator at $\mathcal{AI}_n(f)$ and the other one has minimum degree annihilator at degree $> \mathcal{AI}_n(f)$. Then there is no $fg = h$ relation having $\deg(h) = \mathcal{AI}_n(f)$ and $\deg(g) < \mathcal{AI}_n(f)$.*

We also present the following result that can be used to find minimum degree g in the relation $fg = h$, where $\deg(h) = \mathcal{AI}_n(f)$.

Proposition 3. *Consider that $f, 1+f$ have minimum degree annihilators at the same degree $\mathcal{AI}_n(f)$ and let h be a function at that degree. Let A be the set of annihilators of f and B be the set of annihilators of $1+f$ at degree $\mathcal{AI}_n(f)$. Then the minimum degree of g such that $fg = h$ is $\min_{\beta_A \in A, \beta_B \in B} \deg(\beta_A + \beta_B)$.*

Also we present the following technical relation relating g and h only.

Proposition 4. *If $fg = h$, then $gh = h$, i.e., g is the annihilator of $1+h$.*

Proof. We have, $fg = h$, i.e., $fgg = gh$, i.e., $fg = gh$, i.e., $h = gh$. □

Consider two functions $\tau_1, \tau_2 \in B_n$ having full algebraic immunity $\lceil \frac{n}{2} \rceil$ when n is odd. If we consider the function $\tau = (1+x_{n+1})\tau_1 + x_{n+1}\tau_2$, on even number of variables, it can be checked using [21, Proposition 1(2)] that this is again of full algebraic immunity $\frac{n+1}{2}$ which is actually $\lceil \frac{n}{2} \rceil$.

However, the situation is not as simple when we take n even. In such a situation we start with two functions $\tau_1, \tau_2 \in B_n$ having full algebraic immunity $\frac{n}{2}$. In that case, $\tau = (1 + x_{n+1})\tau_1 + x_{n+1}\tau_2$, on odd number of variables may or may not have full algebraic immunity $\lceil \frac{n+1}{2} \rceil = \frac{n}{2} + 1$.

Consider τ_1, τ_2 have annihilators π_1, π_2 at degree $\frac{n}{2}$ and $1 + \tau_1, 1 + \tau_2$ have annihilators π'_1, π'_2 at degree $\frac{n}{2}$. Then following [21, Proposition 1(2)], τ will have algebraic immunity $\frac{n}{2}$, iff $\deg(\pi_1 + \pi_2) < \frac{n}{2}$ or $\deg(\pi'_1 + \pi'_2) < \frac{n}{2}$.

Now consider that τ_1, τ_2 have minimum degree annihilators π_1, π_2 at degree $\frac{n}{2}$ and $\frac{n}{2} + 1$ respectively. Further $1 + \tau_1, 1 + \tau_2$ have minimum degree annihilators π'_1, π'_2 at degree $\frac{n}{2} + 1$ and $\frac{n}{2}$ respectively. Then one can check that τ has algebraic immunity $\frac{n}{2} + 1$. Note that the functions ϕ_{2k} (in Section 2) and the functions ψ_{2k} (in Section 3) have the properties like τ_1 and $1 + \phi_{2k}$, $1 + \psi_{2k}$ have the properties like τ_2. Thus the availability of the functions ϕ_{2k}, ψ_{2k} having full algebraic immunity k presents a clear construction using them to get functions with full algebraic immunity $k + 1$ on odd number of variables $2k + 1$. As concrete examples, $x_{2k+1} + \phi_{2k}$, $x_{2k+1} + \psi_{2k}$, $(1 + x_{n+1})\phi_{2k} + x_{n+1}(1 + \psi_{2k})$, $(1 + x_{n+1})\psi_{2k} + x_{n+1}(1 + \phi_{2k})$ are functions on odd number of variables with full algebraic immunity.

Proposition 5. *Suppose $f \in B_{2k}$ for $k \geq 0$ such that f and $1 + f$ have no annihilator of degree $< k$ and $< k+1$ respectively. Then $wt(f) = 2^{2k-1} - \binom{2k-1}{k}$.*

Proof. Since f and $1 + f$ have no annihilator of degree $< k$ and $< k + 1$ respectively, following the proof of [21, Theorem 1] we have $wt(f) \geq \sum_{i=0}^{k-1} \binom{2k}{i}$ and $wt(1+f) \geq \sum_{i=0}^{k} \binom{2k}{i}$. This implies $wt(f)$ is exactly $\sum_{i=0}^{k-1} \binom{2k}{i} = 2^{2k-1} - \binom{2k-1}{k}$. □

As a corollary of this result we can get exact weights $2^{2k-1} - \binom{2k-1}{k}$ of ϕ_{2k} and ψ_{2k} which is already given in [13, 23].

2 Study of the construction from [22]

In [22], for the first time functions with full algebraic immunity have been constructed. The construction is as follows.

Construction 1 *Denote by $\phi_{2k} \in B_{2k}$ the function defined by the recursion:*

$$\phi_{2k+2} = \phi_{2k} || \phi_{2k} || \phi_{2k} || \phi^1_{2k}, \tag{1}$$

where $||$ denotes the concatenation. In terms of algebraic normal form, $\phi_{2k+2} = \phi_{2k} + x_{2k+1}x_{2k+2}(\phi_{2k} + \phi^1_{2k})$, and where ϕ^1_{2k} is defined itself by a doubly indexed recursion

$$\phi^i_{2j} = \phi^{i-1}_{2j-2} || \phi^i_{2j-2} || \phi^i_{2j-2} || \phi^{i+1}_{2j-2}, \tag{2}$$

i.e., in terms of algebraic normal form, $\phi^i_{2j} = \phi^{i-1}_{2j-2} + (x_{2j-1} + x_{2j})(\phi^{i-1}_{2j-2} + \phi^i_{2j-2}) + x_{2j-1}x_{2j}(\phi^{i-1}_{2j-2} + \phi^{i+1}_{2j-2})$ for $j > 0$, $i > 0$,

with base step $\phi^0_j = \phi_j$ for $j > 0$, $\phi^i_0 = i \mod 2$ for $i \geq 0$.

What we actually prove now is the minimum degree annihilators of ϕ_{2k} are at the degree k and the the minimum degree annihilators of $1 + \phi_{2k}$ are at the degree $k+1$. Then using Corollary 1, we get that there is no g having degree $< k$ such that $\phi_{2k} g = h$, where $\deg(h) = k$. Note that the proof technique follows the similar line as it has been presented in [22, 13], but there are some necessary technical modifications to get the results.

Lemma 1. *Assume that the function $\phi_{2i} \in B_{2i}$ has been generated by Construction 1 for $0 \le i \le k$ and $f + \phi_{2i}$ has no annihilator of degree $< i+1$ for $0 \le i \le k$ and f is a nonzero function of other variables. If, for some $0 \le i \le k$ and $j \ge 0$, there exist $g \in AN(f + \phi_{2i}^{j})$ and $h \in AN(f + \phi_{2i}^{j+1})$ such that $\deg(g+h) \le i-1-j$ then $g = h$.*

Proof. We prove Lemma 1 by induction on i.

For the base step $i = 0$, $\deg(g+h) \le 0 - 1 - j \le -1$ implies that such a function cannot exist, i.e., $g + h$ is identically 0, which gives $g = h$.

Now we prove the inductive step. Assume that, for $i < \ell$, the induction assumption holds (for every $j \ge 0$). We will show it for $i = \ell$ (and for every $j \ge 0$). Suppose that there exist $g \in AN(f + \phi_{2\ell}^{j})$ and $h \in AN(f + \phi_{2\ell}^{j+1})$ with $\deg(g + h) \le \ell - 1 - j$. By construction, if $j > 0$ then we have

$$\begin{aligned}
\phi_{2\ell}^{j} &= \phi_{2(\ell-1)}^{j-1} || \phi_{2(\ell-1)}^{j} || \phi_{2(\ell-1)}^{j} || \phi_{2(\ell-1)}^{j+1}, \\
\phi_{2\ell}^{j+1} &= \phi_{2(\ell-1)}^{j} || \phi_{2(\ell-1)}^{j+1} || \phi_{2(\ell-1)}^{j+1} || \phi_{2(\ell-1)}^{j+2}
\end{aligned}$$

and if $j = 0$ then

$$\phi_{2\ell}^{0} = \phi_{2(\ell-1)}^{0} || \phi_{2(\ell-1)}^{0} || \phi_{2(\ell-1)}^{0} || \phi_{2(\ell-1)}^{1}.$$

Let us denote

$$\begin{aligned}
g &= v_1 || v_2 || v_3 || v_4, \\
h &= v_5 || v_6 || v_7 || v_8.
\end{aligned}$$

Since $\deg(g + h) \le \ell - 1 - j$, from the ANF of $g + h = (v_1 + v_5) + x_{2\ell-1}(v_1 + v_5 + v_2 + v_6) + x_{2\ell}(v_1 + v_5 + v_3 + v_7) + x_{2\ell-1}x_{2\ell}(v_1 + \cdots + v_8)$ we deduce the following.

- $\deg(v_1 + v_5) \le \ell - 1 - j = (\ell - 1) - 1 - (j - 1)$. If $j > 0$ then $v_1 \in AN(f + \phi_{2(\ell-1)}^{j-1}), v_5 \in AN(f + \phi_{2(\ell-1)}^{j})$ implies that $v_1 = v_5$, according to the induction assumption. If $j = 0$, then we have $v_1, v_5 \in AN(f + \phi_{2(\ell-1)})$, and therefore $(v_1 + v_5) \in AN(f + \phi_{2(\ell-1)})$, with $\deg(v_1 + v_5) \le \ell - 1$. Suppose that $v_1 + v_5 \ne 0$, then we would have $\deg(v_1 + v_5) \ge \ell$, since $f + \phi_{2(\ell-1)})$ has no annihilator of degree $\le \ell - 1$, by hypothesis; a contradiction. Hence $v_1 + v_5 = 0$ i.e. $v_1 = v_5$.
- $\deg(v_2 + v_6) \le (\ell-1) - 1 - j$ and $v_2 \in AN(f + \phi_{2(\ell-1)}^{j}), v_6 \in AN(f + \phi_{2(\ell-1)}^{j+1})$, imply that $v_2 = v_6$, according to the induction assumption.
- $\deg(v_3 + v_7) \le (\ell-1) - 1 - j$ and $v_3 \in AN(f + \phi_{2(\ell-1)}^{j}), v_7 \in AN(f + \phi_{2(\ell-1)}^{j+1})$, imply that $v_3 = v_7$, according to the induction assumption.

– $\deg(v_4 + v_8) \leq (\ell - 1) - 1 - (j + 1)$ and $v_4 \in AN(f + \phi^{j+1}_{2(\ell-1)}), v_8 \in AN(f + \phi^{j+2}_{2(\ell-1)})$, imply that $v_4 = v_8$, according to the induction assumption.

Hence we get $g = h$. □

Lemma 2. *Assume that the function $\phi_{2i} \in B_{2i}$ has been generated by Construction 1 for $0 \leq i \leq k$ and that $f+\phi_{2i}$ where f is a nonzero function other variables has no annihilator of degree $< i + 1$ for $0 \leq i \leq k$. If, for some $0 \leq i \leq k$ and $j \geq 0$, there exists $g \in AN(f + \phi^j_{2i}) \cap AN(f + \phi^{j+1}_{2i})$ such that $\deg(g) \leq i+j+1$, then $g = 0$.*

Proof. We prove Lemma 2 by induction on $i - j$.

For the base step (i.e., $i - j \leq 0$), we have from Construction 1 $f + \phi^{j+1}_{2i} = 1 + f + \phi^j_{2i}$ (this can easily be checked by induction). Hence, $g \in AN(f + \phi^j_{2i}) \cap AN(f + \phi^j_{2i} + 1)$, and $g = 0$.

Now we prove the inductive step. Assume that the induction assumption holds for $i - j \leq \ell$, $\ell \geq 0$, and let us prove it for $i - j = \ell + 1$. So let $g \in AN(f + \phi^j_{2i}) \cap AN(f + \phi^{j+1}_{2i})$ where $i - j = \ell + 1$.

If $j > 0$, we have:

$$\begin{aligned} \phi^j_{2i} &= \phi^{j-1}_{2(i-1)}||\phi^j_{2(i-1)}||\phi^j_{2(i-1)}||\phi^{j+1}_{2(i-1)}, \\ \phi^{j+1}_{2i} &= \phi^j_{2(i-1)}||\phi^{j+1}_{2(i-1)}||\phi^{j+1}_{2(i-1)}||\phi^{j+2}_{2(i-1)}. \end{aligned}$$

Let us denote

$$g = v_1||v_2||v_3||v_4, \text{ we have}$$

$v_1 \in AN(f+\phi^{j-1}_{2(i-1)}) \cap AN(f+\phi^j_{2(i-1)})$, $v_2, v_3 \in AN(f+\phi^j_{2(i-1)}) \cap AN(f+\phi^{j+1}_{2(i-1)})$ and $v_4 \in AN(f + \phi^{j+1}_{2(i-1)}) \cap AN(f + \phi^{j+2}_{2(i-1)})$.

1. Since $\deg(g) \leq i + j + 1$, we have $\deg(v_4) \leq i + j + 1 = (i - 1) + (j + 1) + 1$. Since $(i - 1) - (j + 1) = i - j - 2 < \ell$, we have $v_4 = 0$, according to the induction assumption. So the ANF of g is $v_1 + x_{2i-1}(v_1 + v_2) + x_{2i}(v_1 + v_3) + x_{2i-1}x_{2i}(v_1+v_2+v_3)$. Then $\deg(v_1+v_2), \deg(v_1+v_3), \deg(v_1+v_2+v_3) \leq i+j$, which implies $\deg(v_1), \deg(v_2), \deg(v_3) \leq i + j$.
2. We have then $\deg(v_2) \leq i + j = (i - 1) + j + 1$ and $\deg(v_3) \leq i + j = (i - 1) + j + 1$. Since $(i - 1) - j = i - j - 1 \leq \ell$, we have $v_2 = v_3 = 0$, according to the induction assumption.
3. Since $v_2 = v_3 = v_4 = 0$, the ANF of g is $(1 + x_{2i-1} + x_{2i} + x_{2i-1}x_{2i})v_1$. So, $\deg(v_1) \leq i + j - 1 = (i - 1) + (j - 1) + 1$. Here $(i - 1) - (j - 1) = \ell + 1$. So, we can not use the induction assumption directly. Now we break v_1 again into four parts as

$$\begin{aligned} \phi^{j-1}_{2(i-1)} &= \phi^{j-2}_{2(i-2)}||\phi^{j-1}_{2(i-2)}||\phi^{j-1}_{2(i-2)}||\phi^j_{2(i-2)}, \\ \phi^j_{2(i-1)} &= \phi^{j-1}_{2(i-2)}||\phi^j_{2(i-2)}||\phi^j_{2(i-2)}||\phi^{j+1}_{2(i-2)}, \\ v_1 &= v_{1,1}||v_{1,2}||v_{1,3}||v_{1,4}. \end{aligned}$$

Using similar arguments as in Item 1,2, we have $v_{1,2} = v_{1,3} = v_{1,4} = 0$. So, $\deg(v_{1,1}) \leq i + j - 3$. Doing the similar process j times, we will get some function $v \in AN(f + \phi_{2(i-j)}) \cap AN(f + \phi^1_{2(i-j)})$. At every step of this sub-induction, the degree decreases by 2, and we have then $\deg(v) \leq i + j + 1 - 2j = i - j + 1$. Breaking v a last time into four parts and using that $v \in AN(f + \phi_{2(i-j)}) \cap AN(f + \phi^1_{2(i-j)})$, we have

$$\begin{aligned}\phi_{2(i-j)} &= \phi_{2(i-j-1)}||\phi_{2(i-j-1)}||\phi_{2(i-j-1)}||\phi^1_{2(i-j-1)},\\ \phi^1_{2(i-j)} &= \phi_{2(i-j-1)}||\phi^1_{2(i-j-1)}||\phi^1_{2(i-j-1)}||\phi^2_{2(i-j-1)},\\ v &= v'||v''||v'''||v''''.\end{aligned}$$

Using similar arguments as in Item 1,2, we have $v'' = v''' = v'''' = 0$. So, $\deg(v') \leq i - j - 1$. And $v' \in AN(f + \phi_{2(i-j-1)})$ implies that, if $v' \neq 0$, then $\deg(v) \geq i - j$, a contradiction. Hence, $v' = 0$ which implies $g = 0$.

If $j = 0$, then the proof is similar to the last step in Item 3 above. □

Theorem 1. *Let $f' \in B_{2k+l} = f + \phi_{2k}$ where $f \in B_l$ is a non zero function depends on variables $\{x_{2k+1}, \ldots, x_{2k+l}\}$ and $\phi_{2k} \in B_{2k}$ depends on variables $\{x_1, \ldots, x_{2k}\}$ for $k, l \geq 0$. Then f' has no annihilator of degree $< k + 1$.*

Proof. We prove Theorem 1 by induction on k. For $k = 0$, we have $f' = f$ and hence there is no annihilator of degree < 1. In the inductive step, we assume the hypothesis true until k and we have to prove that any nonzero function g_{2k+2} such that $g_{2k+2}f' = 0$ has degree at least $k + 2$. Suppose that such a function g_{2k+2} with degree $\leq k + 1$ exists. Then, g_{2k+2} can be decomposed as

$$g_{2k+2} = g_{2k}||g'_{2k}||g''_{2k}||h_{2k},$$

where $g_{2k}, g'_{2k}, g''_{2k} \in AN(f+\phi_{2k})$, and $h_{2k} \in AN(f+\phi^1_{2k})$. The algebraic normal form of g_{2k+2} is then $g_{2k+2}(x_1, \ldots, x_{2k+2}) = g_{2k} + x_{2k+1}(g_{2k} + g'_{2k}) + x_{2k+2}(g_{2k} + g''_{2k}) + x_{2k+1}x_{2k+2}(g_{2k} + g'_{2k} + g''_{2k} + h_{2k})$.

If g_{2k+2} has degree $\leq k+1$, then $(g_{2k}+g'_{2k})$ and $(g_{2k}+g''_{2k})$ have degrees $\leq k$. Because both functions lie in $AN(f + \phi_{2k})$ and according induction assumption $f + \phi_{2k}$ has no annihilator of degree $< k + 1$, we deduce that $g_{2k} + g'_{2k} = 0$ and $g_{2k} + g''_{2k} = 0$, which give, $g_{2k} = g'_{2k} = g''_{2k}$. Therefore, $g_{2k+2} = g_{2k} + x_{2k+1}x_{2k+2}(g_{2k}+h_{2k})$, $\deg(g_{2k}) \leq k+1$ and $\deg(g_{2k}+h_{2k}) \leq k-1$. According to Lemma 1, we have $g_{2k} = h_{2k}$. According to Lemma 2, we have then $g_{2k} = h_{2k} = 0$ that gives, $g_{2k+2} = 0$. This completes the proof. □

Remark 1. If $f \in B_l$ (in above theorem) has no annihilator of degree $< t$ where $t \geq 2$, then the question is whether $f + \phi_{2k}$ has no annihilator of degree $< t + k$. In general, the answer is no. Because in the Lemma 1 we have to consider $\deg(g + h) \leq i - 2 - j + t$ and in the base step in the proof of the lemma, i.e., for $i = 0$, $\deg(g + h) \leq -2 - j + t$. So for $j = 0$, $\deg(g + h) \leq t - 2$ where $t - 2 \geq 0$. So, we can not tell that $g + h = 0$. So, it is always true for the case $t \leq 1$, but not for $t \geq 2$.

Corollary 2. *$1 + \phi_{2k}$ has no annihilator of degree $< k+1$, but has annihilator at degree $k+1$.*

Proof. In the Theorem 1, we take $f \in B_0$ is constant 1 function, i.e., the truth table of f contains a single 1. As f is nonzero, following the Theorem 1, $1+\phi_{2k}$ has no annihilator of degree $\leq k$.

From [13], we have $wt(\phi_{2k}) = 2^{2k-1} - \binom{2k-1}{k-1}$. Thus, $wt(1+\phi_{2k}) = 2^{2k-1} + \binom{2k-1}{k-1}$. Then following the proof of [21, Theorem 1], we find that $1+\phi_{2k}$ must have an annihilator at degree $k+1$ as it has the weight $2^{2k-1} + \binom{2k-1}{k-1}$. □

Theorem 2. *Consider $g, h \in B_{2k}$ such that $\phi_{2k} g = h$, where $\deg(h) = k$. Then $\deg(g) \geq k$.*

Proof. Note that for any function on $2k$ variables, either the function or its complement must have an annihilator at degree k. Since $1+\phi_{2k}$ has no annihilator at degree k, ϕ_{2k} must have an annihilator at degree k. Also it is known [22, 13] that ϕ_{2k} has minimum degree annihilator at degree k. Thus the degree of minimum degree annihilator of ϕ_{2k} and $1+\phi_{2k}$ are different, k, $k+1$ respectively. Then the proof follows using Corollary 1. □

Note that this means one cannot get a lower degree (than $\mathcal{AI}_{2k}(\phi_{2k}) = k$) g by fixing h at a degree k. *Note that in [1, Table 3], the functions on $2k$ variables are not ϕ_{2k}, but the functions [22, Example 1] of the form $x_1x_2 + \phi_{2k-2}(x_3, \ldots, x_{2k})$ which are also of full algebraic immunity k. That is why those functions [22, Example 1] are weak against fast algebraic attack.* Further in case of $\deg(h) > k$, we present the following experimental results for the $\phi_{2k} g = h$ relationships for $6 \leq 2k \leq 14$. We present the minimum degree of g in the table till it becomes 1.

$2k$	$\deg(g)$	$\deg(h)$
6	1	4
8	1	5
10	2	6
10	2	7
10	1	8
12	3	7
12	3	8
12	1	9
14	4	8
14	4	9
14	2	10
14	2	11
14	1	12

Table 1. Experimental results on $\phi_{2k} g = h$ relationship.

From Table 1, it is clear that with the increase of $\deg(h)$, the degree of g decreases as expected, but the rate of decrease is not sharp. In fact, if one uses ϕ_{14}, then one gets a linear g only when h is of degree 12. Thus we like to point out that though the function ϕ_{2k} is not good in terms of nonlinearity [13], its structure is good for immunity against both algebraic and fast algebraic attacks.

3 Study on symmetric and rotation symmetric functions

The following construction for symmetric functions with maximum algebraic immunity has been presented in [23, 10]. Consider $\psi_n \in B_n$, as follows:

$$\psi_n(x) = \begin{cases} 1 \text{ for } wt(x) < \lceil \frac{n}{2} \rceil, \\ 0 \text{ for } wt(x) \geq \lceil \frac{n}{2} \rceil. \end{cases}$$

One can check using the proof technique in [23, Lemma 3] that ψ_{2k} has minimum degree annihilator at degree k and $1 + \psi_{2k}$ has minimum degree annihilator at degree $k+1$. This, using Corollary 1, proves that for $g, h \in B_{2k}$ such that $\psi_{2k} g = h$, where $\deg(h) = k$, we will always get $\deg(g) \geq k$. This result has already been proved in a different technique in [9]. Further some interesting $f * g = h$ relationship has been studied in [9, 1].

The algebraic degree of ψ_n is $2^{\lfloor \log_2 n \rfloor}$ [23] and we will always get a constant 1 function g (i.e., of degree 0) such that $\psi_n g = h$, where $\deg(h) = 2^{\lfloor \log_2 n \rfloor}$, i.e., $h = \psi_n$. Similarly extending [9, Theorem 13], if $2^t < n \leq 2^{t+1}$, then there always exist $\psi_n g = h$ relations having $\deg(g) = 1$ and $\deg(h) = 2^t + 1$ (the result in [9, Theorem 13] shows this only when n is a power of 2). Note that the theoretical results given in [1, Table 4] are not tight due to this reason. In Table 2, we present the results in tabular form and this may be compared with Table 1. Based on these, it seems that the ψ_{2k} functions have worse profile than ϕ_{2k}. Note that the weight and nonlinearity of ψ_{2k} and ϕ_{2k} are same, but the algebraic degree of ϕ_{2k} is in general greater than that of ψ_{2k} [23, 13].

$2k$	$\deg(g)$	$\deg(h)$
6	0	4
8	1	5
10	2	6
10	2	7
10	0	8
12	3	7
12	0	8
14	0	8

Table 2. Experimental results on $\psi_{2k} g = h$ relationship.

A more general class of functions with maximum possible algebraic immunity has been proposed in [23].

Construction 2 *Consider $\zeta_{2k} \in B_{2k}$, $k \geq 0$, as follows:*

$$\zeta_{2k}(x) = \begin{cases} 0 \textit{ for } wt(x) < k, \\ a \textit{ for } wt(x) = k, \ a \in \{0, 1\}, \\ 1 \textit{ for } wt(x) > k. \end{cases}$$

Note that if the value of a is same for all the weight k inputs, then it is a symmetric function. However, we will now specifically consider the case where the outputs corresponding to weight k inputs take both the distinct values $0, 1$ and the function becomes non symmetric.

Proposition 6. *Consider ζ_{2k} as described in Construction 2. Then both $\zeta_{2k}, 1 + \zeta_{2k}$ has minimum degree annihilators at degree k.*

Proof. From [23] we already have $\mathcal{AI}_{2k}(\zeta_{2k}) = k$. That both $\zeta_{2k}, 1 + \zeta_{2k}$ has minimum degree annihilators at degree k can be proved considering their weights of $\zeta_{2k}, 1 + \zeta_{2k}$ and following the same kind of arguement as in the proof of [21, Theorem 1]. $\square$

Based on Proposition 6, it is not clear whether there exists g having $\deg(g) < k$ such that $\zeta_{2k} g = h$, where $\deg(h) = k$. Thus we go for the following experimentation. We use similar kind of functions as described in [23] as follows.

$$\begin{aligned} G(x_1, \ldots, x_{2k}) &= 0 \text{ for } wt(x_1, \ldots, x_{2k}) < k, \\ &= 1 \text{ for } wt(x_1, \ldots, x_{2k}) > k, \\ &= b(x_1, \ldots, x_{2k}) \text{ for } wt(x_1, \ldots, x_{2k}) = k, \end{aligned}$$

where $b(x_1, \ldots, x_{2k})$ is a Maiorana-McFarland type bent function.

1. If $wt(G) < 2^{2k-1}$, then we choose $2^{2k-1} - wt(G)$ points randomly from the inputs having weight k and output 0 of G and toggle those outputs to 1 to get ζ_{2k}.
2. If $wt(G) > 2^{2k-1}$, then we choose $wt(G) - 2^{2k-1}$ points randomly from the inputs having weight k and output 1 of G and toggle those outputs to 0 to get ζ_{2k}.

Thus we get balanced ζ_{2k}. As we have already described in Proposition 6, the $fg = h$ relationships for the functions of the type of ζ_{2k} may not be decided immediately. Thus we present some experimental results for this purpose for a randomly chosen ζ_{2k} for each $6 \leq 2k \leq 14$.

$2k$	$nl(\zeta_{2k})$	$\deg(\zeta_{2k})$	$\deg(g)$	$\deg(h)$
6	22	5	3	3
			1	4
8	92	7	3	4
			1	5
10	384	9	4	5
			2	6
			2	7
			1	8
12	1584	11	5	6
			3	7
			3	8
			1	9
14	6470	13	6	7
			4	8
			1	9

Table 3. Profiles for the functions ζ_{2k}.

3.1 Experimental Results on Rotation Symmetric Boolean Functions

We also consider the following rotation symmetric Boolean functions with good cryptographic properties and full algebraic immunity as they have been studied in [21].

First we consider the 7-variable, 2-resilient, nonlinearity 56 rotation symmetric Boolean functions with algebraic immunity 4. There are 12 such functions. For all these functions f, we got $f * g = h$ relationship where g is a linear function and h has degree 4. Thus these functions are not good in resisting fast algebraic attacks.

Next we consider the 8-variable, 1-resilient, nonlinearity 116 rotation symmetric Boolean functions with algebraic immunity 4. There are 6976 such functions. Out of them there are 6080 many functions f, for which we get good profile. For these functions, we get the profile like $\deg(g) = 3, \deg(h) = 4$, $\deg(g) = 2, \deg(h) = 5$ and $\deg(g) = 1, \deg(h) = 6$. In all these cases we fix degree of h and then find the minimum degree g. Thus there exist 8-variable, 1-resilient, nonlinearity 116 rotation symmetric Boolean functions where we get good profile in terms of fast algebraic attack. Further note that these functions are of degree 6 by itself. The truth table of one of these functions is as below in hexadecimal format:

```
0005557337726F4A1E6E7B4C3CAB7598
03FD7CB86ADA61F41FE48C9E7A26C280
```

3.2 Experimental Results on (Modified) Balanced Patterson-Wiedemann type Functions

Patterson and Wiedemann [28, 29] considered the Boolean functions on odd number of input variables n and succeeded to find out functions having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd $n \geq 15$. This result is pioneering as this is the first instance when such a high nonlinearity has been demonstrated and further till date there is no other strategy to get such functions. Later in [26] these functions have been changed heuristically to get highly nonlinear balanced functions. We consider one of the functions presented in [26], which is a balanced function on 15 variables having nonlinearity $16262 > 2^{15-1} - 2^{\frac{15-1}{2}}$. We found that the algebraic immunity of the function we have considered is 7 (not 8, which is the maximum possible for 15-variable functions). Given this function f, we experimented on the $fg = h$ relationships fixing $\deg(h) \geq 7$ and then finding out the minimum degree g. The $(\deg(g), \deg(h))$ relationships for the function f is as follows: (6, 7), (6, 8), (3, 9), (3, 10), (2, 11), (2, 12), (1,13).

References

1. F. Armknecht, C. Carlet, P. Gaborit, S. Kuenzli, W. Meier and O. Ruatta. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. Accepted in Eurocrypt 2006.
2. F. Armknecht and M. Krause. Algebraic Attacks on combiners with memory. In *Advances in Cryptology - CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, pages 162–175. Springer Verlag, 2003.
3. F. Armknecht. Improving Fast Algebraic Attacks. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 65–82. Springer Verlag, 2004.

4. L. M. Batten. Algebraic Attacks over GF(q). In *Progress in Cryptology - INDOCRYPT 2004*, pages 84–91, number 3348, Lecture Notes in Computer Science, Springer-Verlag.
5. A. Botev. On algebraic immunity of some recursively given sequence of correlation immune functions. In Proceedings of *XV international workshop on Synthesis and complexity of control systems*, Novosibirsk, October 18-23, 2004, pages 8-12 (in Russian).
6. A. Botev. On algebraic immunity of new constructions of filters with high nonlinearity. In Proceedings of *VI international conference on Discrete models in the theory of control systems*, Moscow, December 7-11, 2004, pages 227-230 (in Russian).
7. A. Botev and Y. Tarannikov. Lower bounds on algebraic immunity for recursive constructions of nonlinear filters. Preprint 2004.
8. A. Braeken, J. Lano, N. Mentens, B. Preneel and I. Verbauwhede. SFINKS: A Synchronous stream cipher for restricted hardware environments. SKEW - Symmetric Key Encryption Workshop, 2005.
9. A. Braeken, J. Lano and B. Preneel. Evaluating the Resistance of Filters and Combiners Against Fast Algebraic Attacks. Eprint on ECRYPT, 2005.
10. A. Braeken and B. Preneel. On the Algebraic Immunity of Symmetric Boolean Functions. In *Indocrypt 2005*, number 3797 in LNCS, pages 35–48. Springer Verlag, 2005. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/245, 26 July, 2005.
11. C. Carlet. Improving the algebraic immunity of resilient and nonlinear functions and constructing bent functions. IACR ePrint server, http://eprint.iacr.org, 2004/276. See also the extended abstract entitled "Designing bent functions and resilient functions from known ones, without extending their number of variables" in the proceedings of ISIT 2005.
12. C. Carlet. A lower bound on the higher order nonlinearity of algebraic immune functions. Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2005/469.
13. C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. Submitted to IEEE-IT. This is a revised and extended version of [21, 22].
14. C. Carlet and P. Gaborit. On the construction of balanced Boolean functions with a good algebraic immunity. Proceedings of BFCA (First Workshop on Boolean Functions: Cryptography and Applications), Rouen, France, March 2005, pp. 1-14. See also the extended abstract with the same title in the proceedings of ISIT 2005.
15. J. H. Cheon and D. H. Lee. Resistance of S-boxes against Algebraic Attacks. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 83–94. Springer Verlag, 2004.
16. J. Y. Cho and J. Pieprzyk. Algebraic Attacks on SOBER-t32 and SOBER-128. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 49–64. Springer Verlag, 2004.
17. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *Advances in Cryptology - ASIACRYPT 2002*, number 2501 in Lecture Notes in Computer Science, pages 267–287. Springer Verlag, 2002.
18. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - EUROCRYPT 2003*, number 2656 in Lecture Notes in Computer Science, pages 345–359. Springer Verlag, 2003.
19. N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, pages 176–194. Springer Verlag, 2003.

20. N. Courtois. Cryptanalysis of SFINKS. In *ICISC 2005*. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2005/243, 2005.
21. D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. Indocrypt 2004, Chennai, India, December 20–22, pages 92–106, number 3348 in Lecture Notes in Computer Science, Springer Verlag, 2004
22. D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. In *Workshop on Fast Software Encryption, FSE 2005*, pages 98–111, number 3557, Lecture Notes in Computer Science, Springer-Verlag.
23. D. K. Dalai, S. Maitra and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/229, 15 July, 2005. To be published in Designs, Codes and Cryptography.
24. D. H. Lee, J. Kim, J. Hong, J. W. Han and D. Moon. Algebraic Attacks on Summation Generators. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 34–48. Springer Verlag, 2004.
25. M. Lobanov. Tight bound between nonlinearity and algebraic immunity. Cryptology ePrint Archive, Report 2005/441, http://eprint.iacr.org/.
26. S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. *IEEE Transactions on Information Theory*, 48(1):278–284, January 2002.
27. W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In *Advances in Cryptology - EUROCRYPT 2004*, number 3027 in Lecture Notes in Computer Science, pages 474–491. Springer Verlag, 2004.
28. N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983.
29. N. J. Patterson and D. H. Wiedemann. Correction to - the covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-36(2):443, 1990.