Balanced Boolean Functions with (more than) Maximum Algebraic Immunity

Deepak Kumar Dalai and Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 108, INDIA
Email: {deepak_r, subho}@isical.ac.in

Abstract

In this correspondence, construction of balanced Boolean functions with maximum possible algebraic (annihilator) immunity (AI) is studied with an additional property which is necessary to resist fast algebraic attack. The additional property considered here is, given an n-variable (n even) balanced function f with maximum possible AI $\frac{n}{2}$, and given two n-variable Boolean functions g, h such that $fg = h$, if $\deg(h) = \frac{n}{2}$, then $\deg(g)$ must be greater than or equal to $\frac{n}{2}$. Our results can also be used to present theoretical construction of resilient Boolean functions having maximum possible AI.

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

1 Introduction

In recent time, algebraic and fast algebraic attacks have received a lot of interest in cryptographic literature [3, 12, 13, 20]. An important property for Boolean functions to be used in cryptosystems, called algebraic immunity [20, 15] has been evolved in this area. Good algebraic immunity (of a Boolean function used in a cryptosystem) provides certain kind of resistance against algebraic attacks done in a particular way, i.e., using linearization. Further, based on some recent works related to fast algebraic attacks [2, 13, 5, 1], one should concentrate more 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 [14] by mounting an attack on SFINKS [4]. In one of the recent papers [17], the term annihilator immunity is used instead of algebraic immunity.

Let B_n be the set of all Boolean functions $\{0,1\}^n \rightarrow \{0,1\}$ on n input variables. One may refer to [15] for the definitions of truth table, algebraic normal form (ANF), algebraic degree (deg), weight (wt), nonlinearity (nl) and Walsh spectrum of a Boolean function.

It has been shown in [12] 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.*

We are mostly interested in the lowest degree nonzero annihilators.

Definition 2 *Given $f \in B_n$, its algebraic immunity is defined as [15] the minimum degree of all nonzero annihilators of f or $1 + f$, 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 [12] 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 [6, 7, 10, 8, 15, 16, 17, 20, 19] and the first two constructions of Boolean functions having maximum algebraic (annihilator) immunity is presented in [16, 17] (independently, little later, the construction of [17], with more examples of symmetric functions, has been studied in [6]).

Let us now discuss the situation with respect to fast algebraic attack. Take $f \in B_n$ with maximum possible AI $\lceil \frac{n}{2} \rceil$. It may very well happen that $fg = h$, 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 [5, 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. Even after this concept, the necessary condition of using functions with maximum possible AI stays, but one needs to check the profile of the functions for other $fg = h$ relations before using that in a cryptosystem. One should be aware that only checking these $fg = h$ relationships are not sufficient in terms of resistance to (fast) algebraic attacks as there are number of scenarios to mount algebraic and fast algebraic attacks which are available in details in [12, 13].

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 we will consider $\deg(g) \leq \deg(h)$ for a relation $fg = h$ unless mentioned otherwise.

In this correspondence, we present a specific class of balanced functions f for even number of input variables n having algebraic immunity $\frac{n}{2}$ such that for any $fg = h$ relation if $\deg(h) = \frac{n}{2}$ then $\deg(g)$ cannot be less than $\frac{n}{2}$. This class of functions was not known earlier. Further we show that existence of these functions has direct implication towards existence of resilient functions with maximum possible algebraic immunity. A few important open questions are also raised based on our work. The main contribution of this correspondence is presented in Subsection 2.3.

2 Functions with additional constraint over maximum AI

In this section we consider the functions $f \in B_n$ with maximum possible AI $\lceil \frac{n}{2} \rceil$ with the following property. Given $fg = h$ relation such that $\deg(h) = \lceil \frac{n}{2} \rceil$, $\deg(g) \geq \lfloor \frac{n}{2} \rfloor$. This is the additional constraint. These functions are indeed better than any functions with only maximum AI with respect to fast algebraic attacks since one can not get a g having $\deg(g) < \lfloor \frac{n}{2} \rfloor$ when $\deg(h)$ is fixed at $\lceil \frac{n}{2} \rceil$. This is the best possible case when $\deg(h)$ is fixed at $\lceil \frac{n}{2} \rceil$ as from [13, Theorem 7.2.1], there always exist g, h, such that $fg = h$, with $\deg(g) + \deg(h) \leq n$.

2.1 Some Basic results

First concentrate on functions having full algebraic immunity as presented in [16, 17]. For such a function $f \in B_{2k}$, the lowest degree annihilators are at degree k and for its complement $1 + f$, the lowest degree annihilators are at degree $k + 1$ and hence it can be shown that these functions cannot have $fg = h$ relation such that $\deg(h) = k$ and $\deg(g) < k$. Now one can also check that the $(2k + 1)$-variable function $F = x_{2k+1} + f$ is of algebraic immunity $k + 1$; further F is balanced. One can also check that the function $x_{2k+2} + x_{2k+1} + f$ has algebraic immunity $k + 1$ and it is also an 1-resilient function. We summarize these results below.

Theorem 1

1. *For any even n, it is possible to get unbalanced $f \in B_n$ with maximum possible AI $\frac{n}{2}$ such that given any $fg = h$ relation having* $\deg(h) = \frac{n}{2}$, $\deg(g) \not< \frac{n}{2}$.

2. *For any even n it is possible to get* 1*-resilient function having full algebraic immunity.*

With respect to Theorem 1(1), it is open to get such balanced functions f_b when n is even. We solve this problem in Subsection 2.2 for all even n except when n is an exact power of 2 and then considering $x_{n+1} + f_b$ the corresponding case for Theorem 1(2) will be solved for $n + 1$ (odd) variable functions. Note that experimental evidences of resilient functions with full algebraic immunity are available in [15], but no theoretical result is available in the literature.

Note that the results in Theorem 1 are proved using the functions available in [16, 17] which are of the property that only one of $f, 1 + f$ has minimum degree annihilators at $\mathcal{AI}_n(f)$ and the other one has minimum degree annihilators at degree $1 + \mathcal{AI}_n(f)$. For such functions [18, Proposition 5], $wt(f) = 2^{2k-1} - \binom{2k-1}{k}$ (i.e., these functions are not balanced) and $nl(f) \leq 2^{2k-1} - \binom{2k-1}{k}$.

2.2 Annihilators of $f, 1+f$ at the same degree

Now we will concentrate on the functions such that the minimum degree annihilators of the function and its complement are at the same degree but they never cancel out when added. We formally define this as below.

Definition 3 *Suppose $f \in B_{2k}$ be such that $\mathcal{AI}_{2k}(f) = k$, the maximum possible; the lowest degree annihilators of both f and $1+f$ are at degree k. Further there is no two nonzero k-degree annihilators g and h of f and $1+f$ respectively, such that $\deg(g+h) < k$. We denote such functions by P_{2k} functions.*

Theorem 2 *Suppose f be a P_{2k} function. Then*

1. *$\mathcal{AI}_{2k+1}(x_{2k+1} + f) = k+1$, which is the maximum possible;*
2. *if for $f_1, f_2 \in B_{2k}$, $ff_1 = f_2$ where $\deg(f_1) \leq \deg(f_2) = k$ then $\deg(f_1) = k$;*
3. *$nl(f) \geq 2^{2k-1} - \binom{2k-1}{k-1}$.*

Proof : Let us denote $F = x_{2k+1} + f$. Any nonzero annihilator of F is of the form $g_1 + x_{2k+1}(g_1 + g_2)$, where $g_1 \in AN(f)$ and $g_2 \in AN(1+f)$ and both g_1, g_2 are not 0 at the same time. Similarly any nonzero annihilator of $1+F$ is of the form $g_2 + x_{2k+1}(g_1 + g_2)$. As $g_1 \neq g_2$ and their highest degree terms can not cancel out in $g_1 + g_2$, their degree of the annihilators can not be $\leq k$. Thus $\mathcal{AI}_{2k+1}(F) = k+1$.

Now we prove item 2. Consider we have some f_1, f_2 such that $ff_1 = f_2$ with $\deg(f_1) \leq k$, $\deg(f_2) = k$. Note that $ff_1 = f_2$ iff $f(f_1 + f_2) = 0$ and $(1+f)f_2 = 0$ [5]. So, $f_1 = (f_1 + f_2) + f_2$ is the sum of the two k degree annihilators $f_1 + f_2$ and f_2 of f and $1+f$ respectively. As their highest degree terms never cancel out we have $\deg(f_1) = k$.

Next we prove the last item. Since $x_{2k+1} + f$ is of full algebraic immunity $k+1$, following [19, Corollary 1], one gets $nl(x_{2k+1} + f) \geq 2^{2k} - \binom{2k}{k}$. As for every $2k$-variable function f, we have $nl(x_{2k+1} + f) = 2nl(f)$, we get $nl(f) \geq 2^{2k-1} - \binom{2k-1}{k-1}$. ■

This kind of function provides the best possible relationship when we use functions f on n variables and consider $fg = h$ relationship with $\deg(h) = \frac{n}{2}$ as in that case $\deg(g)$ can not be less than $\frac{n}{2}$. This is the optimum situation when $\deg(h) = \frac{n}{2}$.

Now consider the following construction from [17, 18].

Construction 1 *Consider $\zeta_{2k} \in B_{2k}$, $k \geq 0$, as follows:*

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

We will specifically consider the case where the outputs a_x corresponding to weight k inputs take both the distinct values $0, 1$ and the function becomes non symmetric. One can get a balanced $\zeta_{2k}(x)$ if the outputs corresponding to half of the weight k inputs are 0 and the outputs corresponding to half of the weight k inputs are 1.

Note that there are $\binom{\binom{2k}{k}}{\frac{1}{2}\binom{2k}{k}}$ many balanced functions of the form ζ_{2k} in Construction 1. From $\zeta_{2k}(x)$, the following construction is attempted [17, 18] to get balanced functions.

Construction 2

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

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 one gets balanced ζ_{2k}.

Now we like to point out the problems with the Constructions 1, 2 where the annihilators of f and $1 + f$ are at the same degree.

1. The constructions are randomized and hence the exact nonlinearity of the functions cannot be calculated. In fact, the experimental results show that the nonlinearity of the functions are slightly less than $2^{2k-1} - \binom{2k-1}{k-1}$.

2. Experimental results [18, Table 3] show that there exists g having $\deg(g) < k$ such that $\zeta_{2k} g = h$, where $\deg(h) = k$.

We solve these problems in the construction presented in the following subsection where the functions will have nonlinearity not less than $2^{2k-1} - \binom{2k-1}{k-1}$ and there cannot be any $\deg(g) < k$.

2.3 The exact construction

We present the following construction.

Construction 3 *Consider $\eta_{2k} \in B_{2k}$, as follows:*

$$\eta_{2k}(x) = \begin{cases} 1 \textit{ for } wt(x) < k, \\ a_x \textit{ for } wt(x) = k, \ a_x \in \{0, 1\}, \ \textit{with the constraint } a_x = a_{\overline{x}}, \\ 0 \textit{ for } wt(x) > k, \end{cases}$$

where $\overline{x}$ is the bitwise complement of the vector x. Further all the a_x's are not same, i.e., they take both the values $0, 1$.

Theorem 3 *The functions $\eta_{2k}(x)$ as in Construction 3 are P_{2k} functions.*

Proof : Using the similar proof technique used in [17, Theorem 1], one gets that both η_{2k} and $1+\eta_{2k}$ has no annihilators at degree less than k. Further, $\sum_{i=0}^{k}\binom{n}{i}$ is greater than both $wt(\eta_{2k})$ and $wt(1+\eta_{2k})$ and hence from [15, Theorem 1], both η_{2k} and $1+\eta_{2k}$ must have annihilator at degree less than or equal to k. Hence both $\eta_{2k}(x)$ and $1+\eta_{2k}(x)$ have minimum degree annihilators exactly at degree k.

Any k degree function $g \in B_{2k}$ can be written as

$$a_0 + \sum_{i=0}^{n} a_i x_i + \cdots + \sum_{1\leq < i_1 < \cdots < i_k \leq n} a_{i_1,\ldots,i_k} x_{i_1} \ldots x_{i_k},$$

where the coefficients a's are either 0 or 1. If g is an annihilator of η_{2k} then $g(x)=0$ when $\eta_{2k}(x)=1$. Since $\eta_{2k}(x)=1$ for $wt(x)<k$, we can eliminate all the coefficients (a's) associated to monomials of degree $\leq k-1$ of g. Then we have $\eta_{2k}(x)=1$ for some input vectors x of weight k. For such an $x=(b_1,\ldots,b_n)$, where $b_{i_1}=\cdots=b_{i_k}=1$ and rest 0, one can eliminate the coefficient $a_{i_1,\ldots,i_k}$. Thus the k degree independent annihilators of η_{2k} form the set $S_1=\{x_{j_1}\ldots x_{j_k} : \eta_{2k}(b_1,\ldots,b_n)=0 \text{ and } b_{j_1}=\cdots=b_{j_k}=1, \text{ rest are } 0\}$. Here any k-degree annihilator of η_{2k} does not contain any monomial of degree $<k$.

Define $f'(x)=1+\eta_{2k}(\overline{x})$. Following the similar proof for $\eta_{2k}(x)$, one can prove that the space of k degree annihilators of f' is generated by the basis set $\{x_{j_1}\ldots x_{j_k} : f'(b_1,\ldots,b_n)=0 \text{ and } b_{j_1}=\cdots=b_{j_k}=1, \text{ rest are } 0\}$. Hence, the k degree annihilator space of $f'(\overline{x})=1+\eta_{2k}(x)$ is generated by the basis set $\{(1+x_{j_1})\ldots(1+x_{j_k}) : f'(1+b_1,\ldots,1+b_n)=1+\eta_{2k}(b_1,\ldots,b_n)=0 \text{ and } b_{j_1}=\cdots=b_{j_k}=0, \text{ rest are } 1\}$. So, the subspace of k degree monomials of k degree annihilators of $1+\eta_{2k}$ is generated by the basis set $S_2=\{x_{j_1}\ldots x_{j_k} : \eta_{2k}(b_1,\ldots,b_n)=1 \text{ and } b_{j_1}=\cdots=b_{j_k}=0, \text{ rest are } 1\}$. One can check that these two sets S_1 and S_2 are disjoint iff $\eta_{2k}(x)=\eta_{2k}(\overline{x})$ for $wt(x)=k$.

Since the basis sets S_1, S_2 are disjoint, the k degree terms of any annihilator of η_{2k} and the k degree terms of any annihilator of $1+\eta_{2k}$ cannot be the same. Thus the proof. ■

Corollary 1 *One can get a balanced η_{2k} iff $2k$ is not a power of 2 and the count of such balanced functions is $\binom{\frac{1}{2}\binom{2k}{k}}{\frac{1}{4}\binom{2k}{k}}$.*

Proof : For a $2k$-variable function, there are $\binom{2k}{k}$ many input vectors of weight k and there are $\frac{1}{2}\binom{2k}{k}$ many $(x,\overline{x})$ distinct pairs of weight k. One can construct a balanced η_{2k} if and only if $\frac{1}{2}\binom{2k}{k}$ is even, i.e., $\binom{2k}{k}$ is divisible by 4. Since $\binom{2k}{k}=2\binom{2k-1}{k-1}$, we need to test whether $\binom{2k-1}{k-1}$ is even.

Suppose the $t=\lfloor\log_2 2k\rfloor+1$ bit binary representations of $2k, k, 2k-1$ and $k-1$ are as follows (most significant bit at the left most position):

$$\begin{array}{rcllllllll}
2k & = & b_t & b_{t-1} & \ldots & b_{l+1} & b_l=1 & 0 & 0 & \ldots & 0,\\
k & = & 0 & b_t & \ldots & b_{l+2} & b_{l+1} & b_l=1 & 0 & \ldots & 0,\\
2k-1 & = & b_t & b_{t-1} & \ldots & b_{l+1} & 1+b_l=0 & 1 & 1 & \ldots & 1,\\
k-1 & = & 0 & b_t & \ldots & b_{l+2} & b_{l+1} & 1+b_l=0 & 1 & \ldots & 1,
\end{array}$$

where $1 < l \leq t$, $b_i \in \{0, 1\}$ and $b_t = b_l = 1$. Now following Lucas' theorem [11, Page 79] with the prime 2, we have $\binom{2k-1}{k-1} \equiv \binom{b_t}{0}\binom{b_{t-1}}{b_t} \dots \binom{0}{b_{l+1}}\binom{1}{0}\binom{1}{1} \dots \binom{1}{1}$ mod 2. If $2k$ is a power of 2, then $t = l$. So, $\binom{2k-1}{k-1} \equiv \binom{1}{0}\binom{1}{1} \dots \binom{1}{1}$ mod 2, i.e., $\binom{2k-1}{k-1} \equiv 1$ mod 2. Hence $\binom{2k-1}{k-1}$ is odd.

If $2k$ is not a power of 2, then $\binom{2k-1}{k-1} \equiv \binom{b_{t-1}}{b_t} \dots \binom{b_{l+1}}{b_{l+2}}\binom{0}{b_{l+1}}$ mod 2. At some place we will get $b_s = 0$ and $b_{s+1} = 1$ for $l \leq s < t$ because $b_t = 1$. Hence $\binom{2k-1}{k-1}$ is even if $2k$ is not a power of 2.

Thus $\binom{2k}{k}$ is divisible by 4, when $2k$ is not exactly a power of 2. In such a case, there will be $\frac{1}{2}\binom{2k}{k}$ many distinct pairs of $(x, \overline{x})$, where x is a $2k$ bit binary pattern of weight k. One can choose $\frac{1}{4}\binom{2k}{k}$ many distinct pairs and in such inputs of η_{2k}, output 1 is assigned and for the rest of $\frac{1}{4}\binom{2k}{k}$ many distinct pairs of inputs, output 0 is assigned. This provides a balanced η_{2k}. Note that the number of such distinct balanced η_{2k} is $\binom{\frac{1}{2}\binom{2k}{k}}{\frac{1}{4}\binom{2k}{k}}$. ■

Now an important question is whether there exist balanced P_{2k} functions when $2k$ is a power of 2. We have checked that for $2k = 4 = 2^2$, there is no balanced P_4 function by running exhaustive computer program.

2.4 Functions on odd number of input variables

Now let us study the functions f on odd number of input variables $2k+1$ having maximum possible algebraic immunity $k+1$. That is the functions must be balanced. Consider the following balanced symmetric functions [17, 6, 5] on $2k+1$ variables having full algebraic immunity $k+1$.

Construction 4 *Consider* $\tau_{2k+1} \in B_{2k+1}$, *as follows:*

$$\tau_{2k+1}(x) = \begin{cases} 1 \textit{ for } wt(x) \leq k, \\ 0 \textit{ for } wt(x) \geq k+1, \end{cases}$$

We list a few experimental values of minimum degree of g when $\tau_{2k+1}g = h$ and $\deg(h) = k+1$. In the format $< 2k+1, \deg(g), \deg(h) >$ these values are $< 5, 1, 3 >$, $< 7, 1, 4 >$, $< 9, 1, 5 >$, $< 11, 2, 6 >$. Note that the minimum degree of g is substantially less than k and hence the functions τ_{2k+1} are not interesting in resistance against fast algebraic attacks.

To get a better resistance against fast algebraic attack, we are interested about the balanced functions with the following additional property. Given any $fg = h$ relation having $\deg(h) = k+1$, we require that $\deg(g) \geq k$.

We run exhaustive search for $2k+1 = 5$ variable functions and found such functions. One example is the truth table 00000001000101110001101111011111 which is of nonlinearity 10 and algebraic degree 4. Note that there is no nonlinearity 12 function on 5 variables with such property. Existence of such functions for 7 variables onwards is an open question.

References

[1] F. Armknecht, C. Carlet, P. Gaborit, S. Kuenzli, W. Meier and O. Ruatta. Anonymous. 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] 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.

[5] A. Braeken, J. Lano and B. Preneel. Evaluating the Resistance of Filters and Combiners Against Fast Algebraic Attacks. Eprint on ECRYPT, 2005.

[6] 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.

[7] 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.

[8] C. Carlet. A lower bound on the higher order nonlinearity of algebraic immune functions. Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2005/469.

[9] C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. Accepted in *IEEE Transactions on Information Theory*. This is a revised and extended version of [15, 16].

[10] 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.

[11] L. Comtet. *Advanced combinatorics*, Reidel Publication, 1974.

[12] 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.

[13] 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.

[14] N. Courtois. Cryptanalysis of SFINKS. In *ICISC 2005*. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2005/243, 2005.

[15] 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

[16] 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.

[17] 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.

[18] D. K. Dalai, K. C. Gupta and S. Maitra. Notion of Algebraic Immunity and Its evaluation Related to Fast Algebraic Attacks. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, March 13–15, 2006, LIFAR, University of Rouen, France. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2006/018.

[19] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. Cryptology ePrint Archive, Report 2005/441, http://eprint.iacr.org/.

[20] 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.