New balanced Boolean functions satisfying all the main cryptographic criteria

Claude Carlet*and Keqin Feng †

Abstract

We study an infinite class of functions which provably achieve an optimum algebraic immunity, an optimum algebraic degree and a good nonlinearity. We checked that it has also a good behavior against fast algebraic attacks.

Keywords: Algebraic attack, Boolean function, Stream cipher

1 Introduction

The property needed for resisting the standard algebraic attack of Courtois and Meier [12] is a high algebraic immunity [26]: for a given Boolean function f on n variables, any nonzero Boolean function g such that $f * g = 0$ or $(1 + f) * g = 0$ should have high algebraic degree, where $*$ is the multiplication of functions inherited from multiplication in $\mathbb{F}_2$, the finite field with two elements. The best possible algebraic immunity of n-variable functions is $\lceil \frac{n}{2} \rceil$ [12].
Having a high algebraic immunity is not sufficient for resisting the fast algebraic attacks introduced by Courtois in [10]: if one can find g of low degree and $h \neq 0$ of reasonable degree such that $f * g = h$, then a fast algebraic attack (FAA) is feasible.
Even a high resistance to fast algebraic attacks is not sufficient, since algebraic attacks on the augmented function [19] can be efficient when fast algebraic attacks are not.

There are, up to now, two main infinite classes of Boolean functions achieving optimum algebraic immunity. The first one contains functions in even numbers n of variables and is obtained by an iterative construction. The constructed functions have been further studied in [7], where it is shown that their algebraic degrees are close to n but their

*Claude Carlet is with the Department of Mathematics, University of Paris 8 (MAATICAH), 93526 - Saint-Denis cedex 02, FRANCE; e-mail: claude.carlet@inria.fr.

†Keqin Feng is with the Department of Mathematical Sciences, Tsinghua University, Beijing China 100084; e-mail: kfeng@math.tsinghua.edu.cn. Supported by the NSFC grant 60433050 and the 973 grant of China 2004CB 3180004.

nonlinearity is $2^{n-1} - \binom{n-1}{\frac{n}{2}}$, which is insufficient. Moreover, they are not balanced (but it is possible to build balanced functions from these ones) and are weak against fast algebraic attacks [2, 15]. The second class contains symmetric functions (whose values depend only on the Hamming weight of the input vectors) [3, 15] or functions whose values depend on the Hamming weight of the input vectors except for a few inputs. The nonlinearities of these functions are often not exceeding $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ and when they do exceed it, they are not much greater than this number (see [8]). They are still weaker against fast algebraic attacks [2].

We study an infinite class of functions with optimum algebraic immunity and we show it has good nonlinearity. We show that the functions of this class have also optimum algebraic degree and behave well against fast algebraic attacks. This is the first time a function (and moreover a whole infinite class of functions) is shown to satisfy all of the main criteria for being used as a filtering function in a stream cipher.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$, and B_n the set of n-variable (Boolean) functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The *Hamming weight* $\mathrm{wt}(f)$ of a Boolean function $f \in B_n$ is the size of the support $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ of the function. The *Hamming distance* $\mathrm{d_H}(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference $f + g$ (by abuse of notation, we use $+$ to denote the addition on $\mathbb{F}_2$, i.e., the XOR). We say that a Boolean function f is *balanced* if its truth table contains an equal number of 1's and 0's, that is, if its Hamming weight equals 2^{n-1}.

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF), of the special form:

$$f(x_1, \cdots, x_n) = \sum_{I \subseteq \{1,2,\cdots,n\}} a_I \prod_{i \in I} x_i.$$

The *algebraic degree*, $\deg(f)$, is the global degree of this polynomial, that is, the number of variables in the highest order term with non zero coefficient. A Boolean function is affine if it has degree at most 1. The set of all affine functions is denoted by A_n.

We shall need another representation of Boolean functions, by univariate polynomials over the field $\mathbb{F}_{2^n}$. We identify the field $\mathbb{F}_{2^n}$ and the vector space $\mathbb{F}_2^n$: this field being an n-dimensional $\mathbb{F}_2$-vector space, we can choose a basis $(\beta_1, \cdots, \beta_n)$ and identify every element $x = \sum_{i=1}^{n} x_i \beta_i \in \mathbb{F}_{2^n}$ with the n-tuple of its coordinates $(x_1, \cdots, x_n) \in \mathbb{F}_2^n$. Every function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ (and in particular every Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$) can then be uniquely represented as a polynomial $\sum_{j=0}^{2^n-1} a_j x^j$ where $a_j \in \mathbb{F}_{2^n}$. The function is Boolean if and only if the functions $f(x)$ and $(f(x))^2$ are represented by the

same polynomial, that is, if $a_0, a_{2^n-1} \in \mathbb{F}_2$ and, for every $i = 1, \cdots, 2^n - 2$, we have $a_{2j} = (a_j)^2$, where $2j$ is taken mod $2^n - 1$. Then the algebraic degree of the function equals the maximum *2-weight* $w_2(j)$ of j such that $a_j \neq 0$, where the 2-weight of j equals the number of 1's in its binary expansion. Any Boolean function should have high algebraic degree to allow the cryptosystem resisting the Berlekamp-Massey attack [18].

Boolean functions used in cryptographic systems must have high nonlinearity to withstand fast correlation attacks (see e.g. [6]). The *nonlinearity* of an n-variable function f is its distance from the set of all n-variable affine functions, i.e.,

$$nl(f) = \min_{g \in A_n} (\mathrm{d_H}(f, g)).$$

This parameter can be expressed by means of the Walsh transform. Let $x = (x_1, \cdots, x_n)$ and $\lambda = (\lambda_1, \cdots, \lambda_n)$ both belong to $\mathbb{F}_2^n$ and $\lambda \cdot x$ be the usual inner product in $\mathbb{F}_2^n$: $\lambda \cdot x = \lambda_1 x_1 + \cdots + \lambda_n x_n \in \mathbb{F}_2$, or any other inner product in $\mathbb{F}_2^n$. Let $f(x)$ be a Boolean function in n variables. The *Walsh transform* (depending on the choice of the inner product) of $f(x)$ is the integer valued function over $\mathbb{F}_2^n$ defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\lambda \cdot x}.$$

If we identify the vector space $\mathbb{F}_2^n$ with the field $\mathbb{F}_{2^n}$, then we can take for inner product: $\lambda \cdot x = tr(\lambda x)$.
A Boolean function f is balanced if and only if $W_f(0) = 0$. The nonlinearity of f can also be given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |W_f(\lambda)|.$$

For every n-variable function f we have $nl(f) \leq 2^{n-1} - 2^{n/2-1}$.

For an n-variable Boolean function f, different scenarios related to low degree multiples of f have been studied in [12, 26]. This led to the following definition.

Definition 1 *For $f \in B_n$, define $AN(f) = \{g \in B_n \,|\, f * g = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f. The algebraic immunity (AI) of f is the minimum degree of all the nonzero annihilators of f and of all those of $f + 1$. We denote it by $AI(f)$.*

As shown in [12], we have $AI(f) \leq \lceil \frac{n}{2} \rceil$.

If a function has optimal algebraic immunity $\left\lceil \frac{n}{2} \right\rceil$ with n odd, then it is balanced (see e.g. [7]). Whatever is n, a high value of $AI(f)$ automatically implies that the nonlinearity is not very low: M. Lobanov has obtained in [24] the following tight lower bound:

$$nl(f) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}.$$

However, this bound does not assure that the nonlinearity is high enough. Some functions exhibited in [8] have better nonlinearities but the increasement is not sufficient.

A high algebraic immunity is a necessary but not sufficient condition for robustness against all kinds of algebraic attacks. Indeed, if one can find g of low degree and $h \neq 0$ of reasonable degree such that $f*g = h$, then a fast algebraic attack is feasible, see [10, 1, 20] (note however that fast algebraic attacks need more data than standard ones). This has been exploited in [11] to present an attack on SFINKS [4] and we can say that with this attack, which comes in addition to the standard algebraic attack, Courtois has made very difficult the work of the designer. Since $f * g = h$ implies $f * h = f * f * g = f * g = h$, we see that h is then an annihilator of $f + 1$ and its degree is then at least equal to the algebraic immunity of f. An n-variable function f can be considered as optimal with respect to fast algebraic attacks if there do not exist two functions $g \neq 0$ and h such that $f * g = h$ and $\deg(g) + \deg(h) < n$ with $\deg(g) < n/2$. The question of the existence of such functions was completely open until the present paper.

The pseudo-random generator must also resist algebraic attacks on the augmented function [19], that is, the vectorial function $F(x) = (f(x), f(L(x)), \cdots, f(L^{m-1}(x)))$, where L is the (linear) update function of the linear part of the generator. Algebraic attacks can be more efficient when applied to the augmented function rather than to the function f itself. The efficiency of the attack depends not only on the function f, but also on the update function (and naturally also on the choice of m), since for two different update functions L and L', the vectorial functions $F(x)$ and $F'(x) = (f(x), f(L'(x)), ..., f(L'^{m-1}(x))$ are not linearly equivalent (neither equivalent in the more general sense called CCZ-equivalence, that is, affine equivalence of the graphs of the functions). Testing the behavior of a function with respect to this attack is therefore a long term work (all possible update functions have to be investigated).

Finally, a new version of algebraic attack has been found recently by S. Rønjom and T. Helleseth [29] and is very efficient. Its time complexity is roughly $O(\mathcal{D})$, where $\mathcal{D} = \sum_{i=0}^{\deg(f)} \binom{N}{i}$, where N is the size of the linear part of the pseudo-random generator. But it needs much more data than standard algebraic attacks: $O(\mathcal{D})$ also! When f has degree close to n and algebraic immunity close to $\frac{n}{2}$, this is the square of what is needed by standard algebraic attacks. However, this attack obliges the designer to choose a function with very high degree.

3 The infinite class and its algebraic immunity

Theorem 1 *Let n be any positive integer and α a primitive element of the field F_{2^n}. Let f be the Boolean function on $\mathbb{F}_{2^n}$ whose support is $\{0, 1, \alpha, \cdots, \alpha^{2^{n-1}-2}\}$. Then f has optimum algebraic immunity $\lceil n/2 \rceil$.*

Proof.
Let g be any Boolean function of algebraic degree at most $\lceil n/2 \rceil - 1$. Let $g(x) = \sum_{i=0}^{2^n-1} g_i x^i$ be its univariate representation in the field $\mathbb{F}_{2^n}$, where $g_i \in \mathbb{F}_{2^n}$ is null if the 2-weight $w_2(i)$ of i is at least $\lceil n/2 \rceil$ (which implies in particular that $g_{2^n-1} = 0$).
If g is an annihilator of f, then we have $g(\alpha^i) = 0$ for every $i = 0, \cdots, 2^{n-1} - 2$, that is, the vector $(g_0, \cdots, g_{2^n-2})$ belongs to the Reed-Solomon code over $\mathbb{F}_{2^n}$ of zeroes $1, \alpha, \cdots, \alpha^{2^{n-1}-2}$ (see [25]). According to the BCH bound, if g is non-zero, then this vector has Hamming weight at least 2^{n-1}. Moreover, suppose that the vector $(g_0, \cdots, g_{2^n-2})$ has Hamming weight 2^{n-1} exactly. Then n is odd and $g(x) = \sum_{\substack{0 \le i \le 2^n-2 \\ w_2(i) \le (n-1)/2}} x^i$; but this contradicts the fact that $g(0) = 0$. We deduce that the vector $(g_0, \cdots, g_{2^n-2})$ has Hamming weight strictly greater than 2^{n-1}, leading to a contradiction with the fact that g has algebraic degree at most $\lceil n/2 \rceil - 1$, since the number of integers of 2-weight at most $\lceil n/2 \rceil - 1$ is not strictly greater than 2^{n-1}.
Let g be now a non-zero annihilator of $f + 1$. The vector $(g_0, \cdots, g_{2^n-2})$ belongs then to the Reed-Solomon code over $\mathbb{F}_{2^n}$ of zeroes $\alpha^{2^{n-1}-1}, \cdots, \alpha^{2^n-2}$. According to the BCH bound, this vector has then Hamming weight strictly greater than 2^{n-1}. We arrive to the same contradiction. Hence, there does not exist a non-zero annihilator of f or $f + 1$ of algebraic degree at most $\lceil n/2 \rceil - 1$ and f has then (optimum) algebraic immunity $\lceil n/2 \rceil$. □

4 Algebraic degree and nonlinearity of the function

Theorem 2 *The univariate representation of the function f of Theorem 1 equals*

$$1 + \sum_{i=1}^{2^n-2} \frac{\alpha^i}{(1+\alpha^i)^{1/2}} x^i \tag{1}$$

where $u^{1/2} = u^{2^{n-1}}$. Hence, f has algebraic degree $n-1$ (which is optimum for a balanced function).

Proof. Let $f(x) = \sum_{i=0}^{2^n-1} f_i x^i$ be the univariate representation of f. We have $f_0 =$

$f(0) = 1$, $f_{2^n-1} = 0$ (since f has even Hamming weight) and for every $i \in \{1, \cdots, 2^n-2\}$:

$$f_i = \sum_{j=0}^{2^n-2} f(\alpha^j)\,\alpha^{-ij} = \sum_{j=0}^{2^{n-1}-2} \alpha^{-ij} = \frac{1+\alpha^{-i(2^{n-1}-1)}}{1+\alpha^{-i}} =$$

$$\left(\frac{1+\alpha^{-i(2^n-2)}}{1+\alpha^{-2i}}\right)^{1/2} = \left(\frac{1+\alpha^i}{1+\alpha^{-2i}}\right)^{1/2} = \frac{\alpha^i}{(1+\alpha^i)^{1/2}}.$$

This proves Relation (1). We can see that $f_{2^n-2} \neq 0$ and therefore f has algebraic degree $n-1$. □

Theorem 3 *Let f be defined as in Theorem 1, then:*

$$nl(f) \geq 2^{n-1} - n \cdot \ln 2 \cdot 2^{\frac{n}{2}} - 1.$$

Proof.

$$nl(f) \;=\; 2^{n-1} - \max_{\lambda \in \mathbb{F}_{2^n}^*} |S_\lambda| \tag{2}$$

where

$$S_\lambda = \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{tr(\lambda\alpha^i)} \quad (\lambda \in \mathbb{F}_{2^n}^*) \tag{3}$$

Let $\zeta = e^{\frac{2\pi\sqrt{-1}}{2^n-1}}$ be a primitive root of 1 in the complex field $\mathbb{C}$, χ be the multiplicative character of $\mathbb{F}_{2^n}$ defined by $\chi(\alpha^j) = \zeta^j$ $(0 \leq j \leq 2^n-2)$ and $\chi(0) = 0$. We define the Gauss sum:

$$G(\chi^\mu) = \sum_{x \in \mathbb{F}_{2^n}^*} \chi^\mu(x)(-1)^{tr(x)} \quad (0 \leq \mu \leq 2^n-2)$$

It is well-known (see [23]) that $G(\chi^0) = -1$ and $|G(\chi^\mu)| = 2^{\frac{n}{2}}$ for $1 \leq \mu \leq 2^n-2$. By Fourier transformation we have

$$(-1)^{tr(\alpha^j)} = \frac{1}{2^n-1} \sum_{\mu=0}^{2^n-2} G(\chi^\mu)\overline{\chi}^\mu(\alpha^j) \quad (0 \leq j \leq 2^n-2)$$

Let $\lambda = \alpha^l$ $(0 \leq l \leq 2^n - 2)$ and $q = 2^n$. Then $\overline{\chi}^\mu(\lambda\alpha^i) = \zeta^{-\mu(l+i)}$ and by (3),

$$\begin{aligned} S_\lambda &= \frac{1}{q-1}\sum_{\mu=0}^{q-2} G(\chi^\mu) \sum_{i=\frac{q}{2}-1}^{q-2} \overline{\chi}^\mu(\lambda\alpha^i) \\ &= \frac{1}{q-1}\sum_{\mu=0}^{q-2} G(\chi^\mu) \sum_{i=\frac{q}{2}-1}^{q-2} \zeta^{-\mu(l+i)} \\ &= \frac{1}{q-1}\left(\sum_{\mu=1}^{q-2} G(\chi^\mu)\zeta^{-\mu l}\ \frac{\zeta^{-\mu(\frac{q}{2}-1)}-1}{1-\zeta^{-\mu}} - \frac{q}{2}\right) \end{aligned}$$

Therefore, for $\lambda \in \mathbb{F}_q^*$,

$$|S_\lambda| \leq \frac{1}{q-1}\left(2\sqrt{q}\sum_{\mu=1}^{\frac{q}{2}-1}\left(sin\frac{\pi\mu}{q-1}\right)^{-1} + \frac{q}{2}\right)$$

We have:

$$\begin{aligned} \sum_{\mu=1}^{\frac{q}{2}-1}\left(sin\frac{\pi\mu}{q-1}\right)^{-1} &\leq (q-1)\int_{\frac{1}{2(q-1)}}^{\frac{1}{2}} \frac{dt}{sin\ \pi t} \\ &\leq (q-1)\int_{\frac{1}{2(q-1)}}^{\frac{1}{2}} \frac{dt}{2t} \\ &= \frac{q-1}{2}\ln(q-1) \end{aligned}$$

We get then:

$$|S_\lambda| \leq \frac{1}{q-1}\left(\sqrt{q}\,(q-1)\ln(q-1) + \frac{q}{2}\right) = \sqrt{q}\,\ln(q-1) + \frac{q}{2(q-1)}$$

and by (2)

$$nl(f) \geq 2^{n-1} - n\cdot\ln 2\cdot 2^{\frac{n}{2}} - 1.$$

□

Remark. The lower bound given by Theorem 3 shows that the nonlinearity of our function f is provably considerably better (at least asymptotically) than those of the previously found functions. Moreover, we checked for small values of n that the exact value of $nl(f)$ is much better than what gives this lower bound and seems quite sufficient for resisting fast correlation attacks (for these small values of n, it behaves as $2^{n-1} - 2^{n/2}$).

5 Immunity against fast algebraic attacks

The computer investigations made using Algorithm 2 of [2] suggest the following properties of the class of functions of Theorem 1:

- No nonzero function g of degree at most e and no function h of degree at most d exist such that $f * g = h$, when $(e, d) = (1, n-2)$ for n odd and $(e, d) = (1, n-3)$ for n even. This has been checked for $n \leq 12$ and we conjecture it for every n.
- For $e > 1$, pairs (g, h) of degrees (e, d) such that $e + d < n - 1$ were never observed. Precisely, the non-existence of such pairs could be checked exhaustively for $n \leq 9$ and $e < n/2$, for $n = 10$ and $e \leq 3$ and for $n = 11$ and $e \leq 2$. This suggests that this class of functions, even if not always optimal against fast algebraic attacks, has a very good behavior.

The instance with $n = 9$ turns out to be optimal. To the best of our knowledge, this is the first time where a function with optimum immunity against FAA's can be observed.

Acknowledgement
The authors thank Simon Fischer and Sihem Mesnager for their help in computing the immunities to fast algebraic attacks and the nonlinearities of the function.

References

[1] Armknecht, F.: Improving fast algebraic attacks, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017 pp. 65-82. Springer, Verlag (2004).

[2] Armknecht, F., Carlet, C., Gaborit, P., Künzli, S., Meier,W. and Ruatta, O.: Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. Advances in Cryptology, EUROCRYPT 2006, Lecture Notes in Computer Science 4004 , pp. 147-164, 2006.

[3] Braeken, A., Preneel, B.: On the algebraic immunity of symmetric Boolean functions, Progress in Cryptology–Indocrypt 2004, Lecture Notes in Computer Science, vol. 3797 pp. 35-48. Springer, Verlag (2005).

[4] Braeken, A., Lano, J., Mentens, N., Preneel, B. and Verbauwhede, I.: SFINKS: A Synchronous stream cipher for restricted hardware environments. SKEW - Symmetric Key Encryption Workshop, 2005.

[5] Canteaut, A.: Open problems related to algebraic attacks on stream ciphers, Coding and Cryptography, Lecture Notes in Computer Science, vol. 3969 pp. 120-134. Springer, Verlag (2006).

[6] Canteaut, A., Trabbia, M.: Improved fast correlation attacks using parity-check equations of weight 4 and 5, Advances in Cryptology–EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807 pp. 573-588. Springer (2000).

[7] Carlet, C., Dalai, D.K., Gupta, K.C., Maitra, S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inform. Theory 52(7), 3105-3121 (2006).

[8] Carlet, C., Zeng, X. and Li, C.: Further properties of several classes of Boolean functions with optimum algebraic immunity. Preprint, IACR e-print archive 2007/370.

[9] Cho, J.Y., Pieprzyk, J.: Algebraic attacks on SOBER-t32 and SOBER-128, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017 pp. 49-64. Springer, Verlag (2004).

[10] Courtois, N.: Fast algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology–CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729 pp. 176-194. Springer, Verlag (2003).

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

[12] Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology–Eurocrypt 2003, Lecture Notes in Computer Science, vol. 2656 pp. 345-359. Springer, Verlag (2003).

[13] Courtois, N., Pieprzyk, J.: Cryptanalysis of block ciphers with overdefined systems of equations, Advances in Cryptology–ASIACRYPT 2002, Lecture Notes in Computer Science, vol. 2501 pp. 267-287. Springer, Verlag (2002).

[14] Dalai, D.K., Gupta, K.C., Maitra, S.: Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3557 pp. 98-111. Springer, Verlag (2005).

[15] Dalai, D.K., Maitra, S., Sarkar, S.: Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Des. Codes Cryptogr. 40(1), 41-58 (2006).

[16] Didier, F.: A new upper bound on the block error probability after decoding over the erasure channel. *IEEE Transactions on Information Theory* 52, pp. 4496- 4503, 2006.

[17] Didier, F.: Using Wiedemann's algorithm to compute the immunity against algebraic and fast algebraic attacks. Proceedings of Indocrypt 2006, LNCS 4329, pp. 236-250.

[18] Ding, C., Xiao, G., Shan, W.: The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, vol. 561. Springer, Verlag (1991).

[19] Fischer, S. and Meier, W.: Algebraic Immunity of S-boxes and Augmented Functions. Proceedings of Fast Software Encryption 2007. Lecture Notes in Comput. Sci. 4593, pp. 366-381.

[20] Hawkes, P. and G. Rose, G.: Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers. In M. K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, LNCS 3152*, pp. 390–406. Springer Verlag, 2004.

[21] Lee, D.H., Kim, J., Hong, J., Han, J.W., Moon, D.: Algebraic attacks on summation generators, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017 pp. 34-48. Springer, Verlag (2004).

[22] Li, N., Qi, W.F.: Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, Advances in Cryptology–ASIACRYPT 2006, Lecture Notes in Computer Science, vol. 4284 pp 84-98. Springer (2006).

[23] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachussetts (1983)

[24] Lobanov, M.: Tight bound between nonlinearity and algebraic immunity. Paper 2005/441 in http://eprint.iacr.org/

[25] MacWilliams, F.J., Sloane, N.J.: The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland (1977).

[26] Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of Boolean functions, Advances in Cryptology–EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027 pp. 474-491. Springer, Verlag (2004).

[27] Y.Nawaz, G.Gong, and K.Gupta. Upper Bounds on Algebraic Immunity of Power Functions. Proceeding of Fast Software Encryption 2006, Lecture Notes in Computer Science 4047, pp. 375-389.

[28] Rodier, F.: Asymptotic nonlinearity of Boolean functions. *Designs, Codes and Cryptography*, no 40:1 2006, pp 59-70.

[29] Rønjom, S., Helleseth, T.: A new attack on the filter generator. IEEE Trans. Inform. Theory 53(5) 1752-1758 (2007).