LETTER

A Note on the Algebraic Immunity of the Enhanced Boolean Functions

Deng TANG[†, ††a)], ***Member***

SUMMARY In 2015, Carlet and Tang [Des. Codes Cryptogr. 76(3): 571-587, 2015] proposed a concept called enhanced Boolean functions and a class of such kind of functions on odd number of variables was constructed. They proved that the constructed functions in this class have optimal algebraic immunity if the numbers of variables are a power of 2 plus 1 and at least sub-optimal algebraic immunity otherwise. In addition, an open problem that if there are enhanced Boolean functions with optimal algebraic immunity and maximal algebraic degree $n-1$ on odd variables $n \neq 2^k+1$ was proposed. In this letter, we give a negative answer to the open problem, that is, we prove that there is no enhanced Boolean function on odd $n \neq 2^k+1$ variables with optimal algebraic immunity and maximal algebraic degree $n-1$.

key words: *stream cipher, enhanced Boolean function, balancedness, algebraic immunity*

1. Introduction

Nonlinear Boolean functions play a central role in the security of symmetric-key cryptosystems. The widely accepted properties for a Boolean function to be used in stream ciphers are balancedness (for avoiding statistical dependence between the plaintext and the ciphertext), high nonlinearity (to resist the best affine approximation [1] and the fast correlation attack [2]), high algebraic degree (for allowing resistance to the Berlekamp-Massey algorithm [3] and the Rønjom-Helleseth attack [4]), optimal algebraic immunity (to withstand the standard algebraic attack [5]), and high fast algebraic immunity (to resist fast algebraic attacks [6]). Additionally, the distribution of some vectorial sequences of the form $(s_{i+j_1}, \cdots, s_{i+j_n})$ from the keystream $(s_i)_{i\in\mathbb{N}}$ generated by the pseudo-random generator must be uniform for any tapping sequence, for resisting Anderson's attack [7]. J. Golić [8] observed that if the filter function employed in a filter model has the form $x_1 + f(x_2, \cdots, x_n)$ or $f(x_1, \cdots, x_{n-1}) + x_n$, then the property of uniformity is satisfied for any tapping sequence. It has been later shown that [9] the function must have one of these two forms for having uniformity for any tapping sequence.

During the past fifteen years, the algebraic immunity and fast algebraic immunity are the most infusive criteria on the design of cryptographic Boolean functions, due to the high efficiency of the algebraic and fast algebraic attacks on stream ciphers; the algebraic and fast algebraic attacks have allowed to cryptanalyse some stream ciphers which were previously believed secure. Till date, Boolean functions with optimal algebraic immunity and high fast algebraic immunity have been built in several ways. In the literature, the majority function, which is a subclass of symmetric Boolean functions, is the first class of functions which has been found with optimal algebraic immunity [10], [11]. For odd number of variables n, Qu et al. proved in [12] that there are exactly two symmetric Boolean functions f_m and $f_m + 1$ in symmetric Boolean functions with optimal algebraic immunity $(n+1)/2$. For even number of variables n, except the majority function, some constructions of symmetric Boolean functions with optimal algebraic immunity can be found in [13]–[15]. In 2011, Peng et al. [16] determined all the even-variable symmetric Boolean functions with optimal algebraic immunity. The total number of such symmetric Boolean functions is $(2\mathrm{wt}(n)+1)2^{\lfloor \log_2 n \rfloor}$, where $\mathrm{wt}(n)$ is the Hamming weight of the binary expansion of the integer n. After the optimal algebraic immunity of the majority function was proven, there are many works on the constructions of Boolean functions with optimal algebraic immunity by modifying the majority function, for instance in [10], [17]–[27]. However, the nonlinearities of all found functions are very closed to $2^{n-1} - \binom{n-1}{\lfloor n/2 \rfloor}$, which is almost the worst possible value according to Lobanov's bound [28] and therefore they are not suitable for the cryptographic use in stream ciphers. In 2008, Carlet and Feng [29] studied an infinite class of n-variable balanced Boolean functions with optimal algebraic immunity. This class had already been studied for its nonlinearity (only) in [30] and it was the single-output case of a construction of vectorial Boolean functions introduced in [31]. It was the first class of Boolean functions almost satisfying all the criteria and potentially satisfying them completely. Inspired by the work of Carlet and Feng, many works on the Boolean functions with optimal algebraic immunity defined over finite field have been done, see for instance Ref. [32]–[36]. It should be noted that the balanced functions in [34] are very weak against fast algebraic attacks (see [37]–[39]) and so cannot be used. There are also some other methods to construct Boolean functions achieving optimal algebraic immunity, for an example, recursive constructions have been proposed in [40].

In [41], the function of the form $f(x_1, \cdots, x_{n-1}) + x_n$ is called the enhanced Boolean function of f.

Manuscript received April 9, 2019.
Manuscript revised August 11, 2019.

[†] The author is with School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China.
[††] The author is with Guangxi Key Laboratory of Cryptography and Information Security, Guilin 541000, China.
a) E-mail: dtang@foxmail.com

DOI: 10.1587/transfun.2019EAL2049

Definition 1 ([41]). *Given any $(n-1)$-variable Boolean function f, the enhanced function $\overline{f} \in \mathcal{B}_n$ is defined as $f(x_1, \cdots, x_{n-1}) + x_n$.*

The authors of [41] studied the relations between the characteristics of a Boolean function and its enhanced function, and they constructed a class of enhanced functions by altering one entry in the truth table of the Carlet-Feng function [29]. The constructed functions have optimal algebraic immunity for even numbers of variables and at least sub-optimal algebraic immunity for odd numbers of variables. Particularly, they proved those functions have optimal algebraic immunity if the numbers of variables is a power of 2 plus 1. In [41, Remark 6], an open problem that if there are enhanced Boolean functions with optimal algebraic immunity and maximal algebraic degree $n-1$ on odd $n \neq 2^k+1$ variables was proposed. In this letter, we prove that there is no enhanced Boolean function on odd $n \neq 2^k+1$ variables with optimal algebraic immunity and maximal algebraic degree $n-1$.

The remainder of this letter is organized as follows. In Sect. 2, the notations and the necessary preliminaries required for the subsequent sections are reviewed. In Sect. 3, we present our main result that there is no enhanced Boolean function on odd $n \neq 2^k+1$ variables having optimal algebraic immunity and maximal algebraic degree $n-1$.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the vector space of n-tuples over the field $\mathbb{F}_2 = \{0,1\}$ of two elements. For any vector $a = (a_1, \cdots, a_n)$ of $\mathbb{F}_2^n$, its Hamming weight $\mathrm{wt}(a)$ is defined as the size of the support $\mathrm{supp}(a) = \{1 \leq i \leq n \mid a_i \neq 0\}$. A Boolean function on n variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Denote by $\mathcal{B}_n$ the set of Boolean functions of n variables. The basic representation of a Boolean function $f(x_1, \cdots, x_n)$ is by its truth table, i.e.,

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

The support of f, denoted by $\mathrm{supp}(f)$, is defined as the set $\{x \in \mathbb{F}_2^n \mid f(x) \neq 0\}$. The Hamming weight $\mathrm{wt}(f)$ of f is the cardinality of the support of f, i.e., $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. We say that the Boolean function $f \in \mathcal{B}_n$ is *balanced* if its Hamming weight equals 2^{n-1}.

Besides, it is well-known that any Boolean function $f \in \mathcal{B}_n$ can be uniquely represented by a multivariate polynomial over $\mathbb{F}_2$, called the algebraic normal form (ANF), namely:

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \Big(\prod_{j=1}^{n} x_j^{u_j} \Big) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u,$$

where $a_u \in \mathbb{F}_2$ and $u = (u_1, \cdots, u_n) \in \mathbb{F}_2^n$. The algebraic degree, denoted by $\deg(f)$, is the maximal value of $\mathrm{wt}(u)$ such that $a_u \neq 0$. A Boolean function is called an affine function if its algebraic degree is at most 1. The set of all affine functions is denoted by A_n. In order to resist the Berlekamp-Massey algorithm [3] and the Rønjom-Helleseth attack [4], Boolean functions used in stream ciphers should have high algebraic degree. It should be noted that the maximum algebraic degree of a balanced Boolean function of n variables is $n-1$.

In order to resist the best affine approximation (BAA) [1] and the fast correlation attack [2], Boolean functions used in a cryptosystem must have high nonlinearity. The nonlinearity $\mathrm{nl}(f)$ of a Boolean function $f \in \mathcal{B}_n$ is defined as

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

where $d_H(f,g)$ is the Hamming distance between f and g, i.e., $d_H(f,g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|$. In other words, the nonlinearity $\mathrm{nl}(f)$ is the minimum Hamming distance between f and all affine functions.

In recent years, algebraic attacks have become a powerful attack which have allowed to cryptanalyse some stream ciphers which were previously believed secure [5]. As a response to the standard algebraic attack, a new cryptographic property for designing Boolean functions used in stream ciphers, called algebraic immunity, has been introduced.

Definition 2 ([42]). *Given two n-variable Boolean functions f and h, we say that h is an annihilator of f if the function fh defined as $(fh)(x) = f(x)h(x)$ is equal to 0. The algebraic immunity $AI(f)$ of a Boolean function f is defined to be the minimum algebraic degree of nonzero Boolean functions h such that h is an annihilator of f or $f+1$.*

To resist the standard algebraic attack, a Boolean function should have algebraic immunity as high as possible. It was proved in [5] that $AI(f) \leq \lceil \frac{n}{2} \rceil$ for an arbitrary n-variable Boolean function f. In this letter, f is said to have optimal algebraic immunity if it achieves the maximum $\lceil \frac{n}{2} \rceil$.

3. Main Result

Let $n \geq 5$ be an odd integer and any enhanced Boolean function $\overline{f} \in \mathcal{B}_n$ with algebraic degree $n-1$. In this section, we will prove that $\overline{f}$ never achieves the maximal algebraic immunity $(n+1)/2$ if n is not equal to a power of 2 plus 1.

We first give some preliminary results which are particularly useful to derive our results.

Lemma 1 ([41], Lemma 1). *For every non-constant Boolean function $f(x_1, \cdots, x_{n-1})$, we have*

$$\mathrm{nl}(\overline{f}) = 2\mathrm{nl}(f) \text{ and}$$
$$\deg(\overline{f}) = \deg(f).$$

Lemma 2 ([41], Lemma 2). *Let f be an $(n-1)$-variable function. Then*

$$AI(f) \leq AI(\overline{f}) \leq AI(f) + 1$$

and $AI(\overline{f}) = AI(f)$ if and only if there exist an annihilator g of f and an annihilator h of $f+1$ such that $\deg(g) = \deg(h) = \deg(g+h) + 1 = AI(f)$.

The following lemma has been directly used in [43] without proof. We give a proof here for the self-completeness of the paper.

Lemma 3. *Let $n \geq 4$ be an even integer. Then we have* $\binom{n-1}{\frac{n}{2}-1} \equiv 1 \pmod 2$ *if and only if n is equal to a power of 2.*

Proof. Note that $\binom{n}{\frac{n}{2}} = 2\binom{n-1}{\frac{n}{2}-1}$. Hence, for proving that $\binom{n-1}{\frac{n}{2}-1} \equiv 1 \pmod 2$ if and only if n is equal to a power of 2, we only need to prove that $\binom{n}{\frac{n}{2}} \equiv 2 \pmod 4$ if and only if n is equal to a power of 2. The expression of binomial coefficients modulo a prime number p is given by Lucas's Theorem (e.g., ([44], p.79)). That is, given two integers a and b and their p-adic representations $a = \sum_{i=0}^{e} a_i p^i$ and $b = \sum_{i=0}^{e} b_i p^i$, then we have

$$\binom{a}{b} \equiv \prod_{i=0}^{e} \binom{a_i}{b_i} \mod p.$$

For $p = 2$, we can see that $\binom{a}{b} \equiv 1 \pmod 2$ if and only if $\forall i, b_i \leq a_i$. Denoted by B_c the coefficient vector $(c_0, c_1, \cdots, c_s)$ of $c = \sum_{i=0}^{s} c_i 2^i$. Assume $B_{\frac{n}{2}-1} = (d_0, d_1, \cdots, d_{e-1}, 0)$, then we have $B_{n-1} = (1, d_0, d_1, \cdots, d_{e-1})$. Then we can easily deduce that $\binom{n-1}{\frac{n}{2}-1} \equiv 1 \pmod 2$ if and only if for every $0 \leq i, j \leq e$ such that $d_i \geq d_j$ and hence $\binom{n}{\frac{n}{2}} \equiv 2 \pmod 4$ if and only if the even $n \geq 4$ is equal to a power of 2. This is the desired conclusion. □

In addition, we need the following lemmas.

Lemma 4 ([43],Theorem 5)**.** *Let $f \in \mathcal{B}_n$ and f_{2^n-1} be the coefficient of the monomial $x_1 x_2 \cdots x_n$ in its ANF. Let e be a positive integer such that $e < n/2$. If $f_{2^n-1} = \binom{n-1}{e} + 1$* mod 2*, then there exists $g \neq 0$ with algebraic degree at most e such that fg has degree at most $n - e - 1$.*

By Lemmas 3 and 4, we have the following corollary.

Corollary 1. *Let $n \geq 3$ be an even integer such that n is not equal to a power of 2 and $f \in \mathcal{B}_n$ be a function which has the property that $AI(f) = n/2$ and $\deg(f) = n$. Then there exists a function $\mu \in \mathcal{B}_n$ with $1 \leq \deg(\mu) \leq n/2 - 1$ such that the algebraic degree of $f\mu$ is $n/2$.*

Proof. According to Lemmas 3 and 4, there exists a nonzero function $\mu \in \mathcal{B}_n$ of algebraic degree at most $n/2 - 1$ such that the algebraic degree of $f\mu$ is at most $n/2$. In addition, we can see that the algebraic degree of $f\mu$ is exact $n/2$ since $AI(f) = n/2$ implies that $\deg(fg) \geq n/2$ for any nonzero function g with algebraic degree strictly less than $n/2$. On the other hand, we have $\deg(\mu) \geq 1$ due to μ is nonzero and $\mu \neq 1$ since $\deg(f\mu) = n$ if $\mu = 1$. This completes the proof. □

We are ready now to present and prove the main results of this letter.

Theorem 1. *Let $n \geq 5$ be an odd integer such that n is not equal to a power of 2 plus 1. There is no enhanced function $\overline{f} \in \mathcal{B}_n$ with $\deg(\overline{f}) = n-1$ such that $\overline{f}$ has optimal algebraic immunity $(n + 1)/2$.*

Proof. Assume that there is an enhanced function $\overline{f} \in \mathcal{B}_n$ such that $\deg(\overline{f}) = n - 1$ and $AI(\overline{f}) = (n + 1)/2$. Note that $\deg(\overline{f}) = n - 1$. Thus, we have $\deg(f) = n - 1$ by Lemma 1. On the other hand, it follows from Lemma 2 that f has optimal algebraic immunity $(n - 1)/2$. Then by Corollary 1, there exists a function $\mu \in \mathcal{B}_n$ with $1 \leq \deg(\mu) \leq (n - 3)/2$ such that the algebraic degree of $f\mu$ is $(n - 1)/2$. Note that $\overline{f}(f\mu + x_n\mu + \mu) = (f + x_n)(f\mu + x_n\mu + \mu) = 0$. Note also that $\deg(f\mu + x_n\mu + \mu) \leq (n - 1)/2$ and $f\mu + x_n\mu + \mu = (f + x_n + 1)\mu \neq 0$. This implies that $\overline{f}$ has a nonzero annihilator $f\mu + x_n\mu + \mu$ with algebraic degree $(n - 1)/2$ which is strictly less than $(n+1)/2$, which is contradict to the assumption that $\overline{f}$ has optimal algebraic immunity $(n+1)/2$. This completes the proof. □

Acknowledgments

We wish to thank the anonymous reviewers for their detailed comments that improved the editorial as well as technical quality of this paper. The first author is supported by the National Natural Science Foundation of China (grants 61602394 and 61872435) and Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201724).

References

[1] C. Ding, G. Xiao, and W. Shan, The Stability Theory of Stream Ciphers, Springer, 1991.
[2] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," Advances in Cryptology–EUROCRYPT 1988, pp.301–314, Springer, 1988.
[3] J. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inf. Theory, vol.15, no.1, pp.122–127, 1969.
[4] S. Ronjom and T. Helleseth, "A new attack on the filter generator," IEEE Trans. Inf. Theory, vol.53, no.5, pp.1752–1758, 2007.
[5] N.T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," Advances in Cryptology–EUROCRYPT 2003, pp.345–359, Springer, 2003.
[6] N.T. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," Advances in Cryptology-CRYPTO 2003, pp.176–194, Springer, 2003.
[7] R. Anderson, "Searching for the optimum correlation attack," Fast Software Encryption, pp.137–143, Springer, 1995.
[8] J.D. Golić, "On the security of nonlinear filter generators," Fast software encryption, pp.173–188, Springer, 1996.
[9] S.V. Smyshlyaev, "Perfectly balanced Boolean functions and golić conjecture," J. Cryptol., vol.25, no.3, pp.464–483, 2012.
[10] 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, pp.41–58, 2006.
[11] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," Progress in Cryptology-INDOCRYPT 2005, pp.35–48, Springer, 2005.
[12] L. Qu, C. Li, and K. Feng, "A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables," IEEE Trans. Inf. Theory, vol.53, no.8, pp.2908–2910, 2007.

[13] A. Braeken, Cryptographic Properties of Boolean Functions and S-Boxes, Ph.D. thesis, Catholic University of Louvain, 2006.

[14] K. Feng, F. Liu, L. Qu, and L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity," IEEE Trans. Inf. Theory, vol.55, no.5, pp.2406–2412, 2009.

[15] Y. Chen and P. Lu, "Two classes of symmetric Boolean functions with optimum algebraic immunity: Construction and analysis," IEEE Trans. Inf. Theory, vol.57, no.4, pp.2522–2538, 2011.

[16] J. Peng, Q. Wu, and H. Kan, "On symmetric Boolean functions with high algebraic immunity on even number of variables," IEEE Trans. Inf. Theory, vol.57, no.10, pp.7205–7220, 2011.

[17] N. Li and W.F. Qi, "Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity," Advances in Cryptology–ASIACRYPT 2006, pp.84–98, Springer, 2006.

[18] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity," Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp.271–280, Springer, 2007.

[19] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," Des. Codes Cryptogr., vol.52, no.3, pp.303–338, 2009.

[20] D. Dong, S. Fu, L. Qu, and C. Li, "A new construction of Boolean functions with maximum algebraic immunity," Information Security, pp.177–185, Springer, 2009.

[21] S. Fu, C. Li, K. Matsuura, and L. Qu, "Construction of rotation symmetric Boolean functions with maximum algebraic immunity," Cryptology and Network Security, pp.402–412, Springer, 2009.

[22] S. Fu, L. Qu, C. Li, and B. Sun, "Balanced rotation symmetric Boolean functions with maximum algebraic immunity," IET Inf. Secur., vol.5, no.2, pp.93–99, 2011.

[23] Y. Li, H. Wang, and H. Kan, "Constructing even-variable symmetric boolean functions with high algebraic immunity," IEICE Trans. Fundamentals, vol.E94-A, no.1, pp.362–366, Jan. 2011.

[24] J. Peng and H. Kan, "Annihilators and algebraic immunity of symmetric Boolean functions," IEICE Trans. Fundamentals, vol.E94-A, no.6, pp.1434–1440, June 2011.

[25] S. Su and X. Tang, "Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity," Des. Codes Cryptogr., vol.71, no.2, pp.183–199, 2014.

[26] S. Su, X. Tang, and X. Zeng, "A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the Reed–Muller code," Des. Codes Cryptogr., vol.72, no.3, pp.653–673, 2014.

[27] J. Peng and H. Kan, "The degree of two classes of 3rd order correlation immune symmetric Boolean functions," IEICE Trans. Fundamentals, vol.E97-A, no.1, pp.365–370, Jan. 2014.

[28] M. Lobanov, "Tight bound between nonlinearity and algebraic immunity," IACR Cryptology ePrint Archive, Report 2005/441, 2005.

[29] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," Advances in Cryptology-ASIACRYPT 2008, pp.425–440, Springer, 2008.

[30] N. Brandstätter, T. Lange, and A. Winterhof, "On the non-linearity and sparsity of Boolean functions related to the discrete logarithm in finite fields of characteristic two," Coding and Cryptography, pp.135–143, Springer, 2006.

[31] K. Feng, Q. Liao, and J. Yang, "Maximal values of generalized algebraic immunity," Des. Codes Cryptogr., vol.50, no.2, pp.243–252, 2009.

[32] Q. Wang, J. Peng, H. Kan, and X. Xue, "Constructions of cryptographically significant Boolean functions using primitive polynomials," IEEE Trans. Inf. Theory, vol.56, no.6, pp.3048–3053, 2010.

[33] 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 Trans. Inf. Theory, vol.57, no.9, pp.6310–6320, 2011.

[34] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," Des. Codes Cryptogr., vol.60, no.1, pp.1–14, 2011.

[35] D. Tang, C. Carlet, and X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," IEEE Trans. Inf. Theory, vol.59, no.1, pp.653–664, 2013.

[36] D. Tang, C. Carlet, X. Tang, and Z. Zhou, "Construction of highly nonlinear 1-resilient Boolean functions with optimal algebraic immunity and provably high fast algebraic immunity," IEEE Trans. Inf. Theory, vol.63, no.9, pp.6113–6125, 2017.

[37] C. Carlet, "On a weakness of the Tu-Deng function and its repair," IACR Cryptology ePrint Archive, Report 2009/606, 2009.

[38] Q. Wang and T. Johansson, "A note on fast algebraic attacks and higher order nonlinearities," Information Security and Cryptology, pp.404–414, Springer, 2010.

[39] Q. Wang, T. Johansson, and H. Kan, "Some results on fast algebraic attacks and higher-order non-linearities," IET Inf. Secur., vol.6, no.1, pp.41–46, 2012.

[40] C. Carlet, D.K. Dalai, K.C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," IEEE Trans. Inf. Theory, vol.52, no.7, pp.3105–3121, 2006.

[41] C. Carlet and D. Tang, "Enhanced Boolean functions suitable for the filter model of pseudo-random generator," Des. Codes Cryptogr., vol.76, no.3, pp.571–587, 2015.

[42] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," Advances in Cryptology-EUROCRYPT 2004, pp.474–491, Springer, 2004.

[43] M. Liu, Y. Zhang, and D. Lin, "Perfect algebraic immune functions," Advances in Cryptology–ASIACRYPT 2012, pp.172–189, Springer, 2012.

[44] L. Comtet, Advanced Combinatorics: The Art of Finite and Infinite Expansions, Springer, 1974.