Dependence of the Algebraic Nonlinearity of 4-Functions of Two Variables from the Cryptographic Properties of Their Component Boolean Functions

Nadiia Kazakova[1], Artem Sokolov[2], and Nataliia Balandina[3]

[1] Odesa State Environmental University, 15 Lvivska str., Odesa, 65016, Ukraine
[2] Odesa Polytechnic National University, 1 Shevchenko ave., Odesa, 65044, Ukraine
[3] National University "Odesa Law Academy", 23 Fontanska road, Odesa, 65000, Ukraine

Abstract

Further development and improvement of the efficiency of ciphers largely depend on the success of solving the problem of synthesizing cryptographic primitives that correspond to the quality criteria both when they are represented by Boolean functions and many-valued logic functions. Among these most significant cryptographic quality criteria are algebraic nonlinearity, distance nonlinearity, error propagation criterion, and correlation immunity criterion. To solve the problem of synthesizing high-quality cryptographic structures, it is important to research the relationship between the level of cryptographic quality of the resulting functions of many-valued logic and their component Boolean functions. In this paper, we represent the results of the research on the algebraic nonlinearity of 4-functions of two variables when they are constructed based on two Boolean functions with given cryptographic quality parameters. The results obtained can be considered as a theoretical basis for improving existing and developing new methods for synthesizing cryptographic primitives, which are characterized by the high cryptographic quality of both component Boolean functions and component many-valued logic functions.

Keywords

Nonlinearity, algebraic normal form, Reed-Muller transform, Reed-Muller-Furrier transform, Boolean function, many-valued logic function.

1. Introduction

Cryptographic methods are the basis for building modern information security systems, which determines the relevance of the task of their further improvement [1, 2]. However, the improvement of cryptographic methods implies not only the search for the optimal structures of ciphers that provide the best implementation of the concepts of diffusion and confusion but also the synthesis of sets of high-quality cryptographic primitives that constitute their basis [3–5].

The task of synthesizing such cryptographic primitives directly depends on chosen methods for estimating the level of their cryptographic quality. Today, to estimate the level of quality of cryptographic primitives, a set of cryptographic quality criteria is used, which is applied to the component Boolean functions of a cryptographic primitive [6] and its component many-valued logic functions. The main criteria for cryptographic quality used are the following: the criterion for maximizing algebraic nonlinearity, the criterion for maximizing distance nonlinearity, the error propagation criterion, and the correlation immunity criterion. These criteria are well-known for Boolean functions [7] and have also been generalized for the case of many-valued logic functions [8]. Moreover, today there is a known integral approach for assessing the cryptographic properties of

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: kaz2003@ukr.net (N. Kazakova); radiosquid@gmail.com (A. Sokolov); nataliabalandina2103@gmail.com (N. Balandina)
ORCID: 0000-0003-3968-4094 (N. Kazakova); 0000-0003-0283-7229 (A. Sokolov); 0000-0002-3121-4517 (N. Balandina)

component many-valued logic functions, which was presented in [9].

Note, that despite the well-known methods for estimating the compliance of Boolean functions and functions of many-valued logic with cryptographic quality criteria, the problem of synthesizing cryptographic primitives of practically valuable lengths that would correspond in the best possible way to these criteria remains unsolved in the general case.

The relationship between the cryptographic quality of component Boolean functions and many-valued logic functions of cryptographic primitive remains understood insufficiently, although both Boolean functions and many-valued logic functions can be considered as different ways of describing the same construction.

In particular, the relationship between the algebraic nonlinearity of a 4-function and the cryptographic quality of its component Boolean functions remains unexplored. This circumstance makes it difficult to further develop methods for synthesizing cryptographic primitives that would have a high level of cryptographic quality when they are represented in all possible ways using many-valued logic functions.

The *purpose* of this paper is to research the relationship between the algebraic nonlinearity of a 4-function and the cryptographic properties of its component Boolean functions.

2. Algebraic Normal Form

The basis of the modern approach for estimating algebraic nonlinearity is the mathematical apparatus of the Algebraic Normal Form (ANF) [10]. The coefficients of terms of the algebraic normal form of Boolean functions of k variables whose truth table length is equal to $N = 2^k$, is found using the Reed-Muller transform

$$A = fL_N,\ f = AL_N, \tag{1}$$

where the direct and inverse Reed-Muller matrices are equal to each other and are determined in accordance with the following recursive relation

$$L_1 = [1],$$
$$L_{2N} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes L_N = \begin{bmatrix} L_N & L_N \\ 0 & L_N \end{bmatrix}, \tag{2}$$

where the symbol $\otimes$ determine the Kronecker product.

In the case of 4-functions, the coefficients of ANF terms can also be found using the Reed-Muller-Fourier transform, which is described in [11], the general form of which can be written as

$$A = L_4 F,\quad F = L_4^{-1} A \tag{3}$$

where the matrices L_4 and L_4^{-1} can be found using the recurrent constructions proposed in [8]

$$L_{4^k}^{-1} = \begin{bmatrix} L_{4^{k-1}}^{-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \\ L_{4^{k-1}}^{-1} & 3L_{4^{k-1}}^{-1} & 2L_{4^{k-1}}^{-1} & L_{4^{k-1}}^{-1} \end{bmatrix},$$
$$L_{4^k} = \begin{bmatrix} L_{4^{k-1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & L_{4^{k-1}} & 3L_{4^{k-1}} & 2L_{4^{k-1}} \\ \mathbf{0} & L_{4^{k-1}} & 2L_{4^{k-1}} & 3L_{4^{k-1}} \\ L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} & L_{4^{k-1}} \end{bmatrix}. \tag{4}$$

Note that in the case of 4-functions, the direct and inverse matrices of the Reed-Muller transform do not coincide, while all arithmetic operations are performed in accordance with the arithmetic of the extended Galois field $GF(4)$.

3. Interconnection Between Cryptographic Properties of Boolean Functions and Algebraic Nonlinearity of 4-Functions

Each 4-function f_4 can be represented as its two component Boolean functions f_{20} and f_{21}, which completely determine its properties, as shown by the following example

f_4	1	1	0	1	1	0	2	3	2	1	3	0	0	0	3	1
f_{20}	1	1	0	1	1	0	0	1	0	1	1	0	0	0	1	1
f_{21}	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	0

. (4)

In this section, we consider the relationship between the cryptographic properties of the component Boolean functions f_{20} and f_{21}, which are parts of the 4-function f_4, and its algebraic degree of nonlinearity.

In case of the necessity to process large sets of Boolean functions, experimental data on the algebraic nonlinearity of 4-functions are obtained in this paper by synthesizing them based on a sample of 10^6 Boolean functions with a given level of cryptographic quality.

3.1. Algebraic Nonlinearity of Component Boolean Functions

The algebraic degree of nonlinearity of a Boolean function is defined as the largest degree of the term of its ANF. For one of the most practically valuable lengths of Boolean functions $N=16$, we represent in the Table 1 the possible terms of the ANF, as well as their algebraic degrees of nonlinearity.

Table 1
Algebraic degrees of ANF terms of Boolean functions of length $N=16$

a_0	x_4	x_3	x_3x_4	x_2	x_2x_4	x_2x_3	$x_2x_3x_4$
0	1	1	2	1	2	2	3
x_1	x_1x_4	x_1x_3	$x_1x_3x_4$	x_1x_2	$x_1x_2x_4$	$x_1x_2x_3$	$x_1x_2x_3x_4$
1	2	2	3	2	3	3	4

In turn, the algebraic degree of nonlinearity of a 4-function is defined as the largest degree of its ANF term, while the possible terms of the ANF, as well as their algebraic degrees of nonlinearity for the 4-function of two variables, are given in Table 2.

Table 2
Algebraic degrees of ANF terms of 4-functions of length $N=16$

a_0	x_2	x_2^2	x_2^3	x_1	x_1x_2	$x_1x_2^2$	$x_1x_2^3$
0	1	2	3	1	2	3	4
x_1^2	$x_1^2x_2$	$x_1^2x_2^2$	$x_1^2x_2^3$	x_1^3	$x_1^3x_2$	$x_1^3x_2^2$	$x_1^3x_2^3$
2	3	4	5	3	4	5	6

To determine the relationship between the ANF of component Boolean functions f_{20}, f_{21} and the constituted by them 4-function f_4, the following experiment was performed. For the selected Boolean functions f_{20} and f_{21} having an equal algebraic degree of nonlinearity (as it is common for component Boolean functions of modern cryptographic algorithms), a 4-function was constructed, for which the algebraic degree of nonlinearity was estimated. The results of the experiment are presented in Table 3. At the same time, in Table 3, the numbers in curly brackets indicate the probabilities of the formation of 4-function f_4 with a given algebraic degree of nonlinearity when using Boolean functions f_{20} and f_{21}, which have a given value of the algebraic degree of nonlinearity.

Table 3
Relationship between algebraic nonlinearity of Boolean functions and 4-functions

$\deg(f_{20})=\deg(f_{21})$	$\deg(f_4)$
0	0 {1.0}
1	1 {0.0667}, 2 {0.9333}
2	2 { $7.9\cdot10^{-4}$ }, 3 {0.2497}, 4 {0.7495}
3	4 {0.0664}, 5 {0.9336}
4	6 {1.0}

Analysis of the data presented in Table 3 allows us to conclude that when combining two Boolean functions of length $N=16$, which have an equal algebraic degree of nonlinearity into one 4-function, the algebraic degree of nonlinearity of the resulting 4-function, in the general case, is not lower than the algebraic degree of nonlinearity of the component Boolean functions.

3.2. Distance Nonlinearity of Component Boolean Functions

Next, we present the results of researching the relationship between the nonlinearity distance of component Boolean functions f_{20}, f_{21} and the 4-function f_4 which is constituted by them.

The nonlinearity distance of a Boolean function is determined as the minimum among its Hamming distances to codewords of an affine code A_j [12], i.e.

$$N_f = \min(dist(f, A_j)), \quad j = 1, 2^{k+1}. \qquad (5)$$

In Table 4 we present the values of the algebraic degree of nonlinearity of the resulting 4-functions, which are constituted by the Boolean functions f_{20} and f_{21}, which have a given level of nonlinearity distance. At the same time, in Table 4, the numbers in curly brackets indicate the probabilities of the formation of 4-function f_4 with a given algebraic degree of nonlinearity when using Boolean functions f_{20} and f_{21}, which have a given value of the nonlinearity distance.

Table 4
Relationship between the nonlinearity distance of Boolean functions and the algebraic nonlinearity of 4-functions

$N_{f_{20}} = N_{f_{21}}$	$\deg(f_4)$
0	0 {0.0039},1 {0.0586}, 2 {0.9375}
1	6 {1.0}
2	4 {0.0664}, 5 {0.9336}
3	6 {1.0}
4	3 { $4.5\cdot10^{-4}$ }, 4 {0.0623}, 5 {0.9372}
5	6 {1.0}
6	2 {0.0038}, 3 {0.2606}, 4 {0.7357}

The analysis of the data presented in Table 4 shows that 4-functions with the largest value of the algebraic degree of nonlinearity can be constituted on the basis of Boolean functions, the nonlinearity distance of which has an odd value.

3.3. Avalanche Characteristics of Component Boolean Functions

To solve practical problems, quite a lot of modifications of the error propagation criterion have been proposed, among which the strict avalanche criterion is the most common and in demand. The correspondence of a Boolean function to a strict avalanche criterion is determined based on the following definition.

Definition 1 [13, 14]. The Boolean function f_2 corresponds to the strict avalanche criterion, if its derivatives $D_u f_2(x) = f_2(x) \oplus f_2(x \oplus u)$ in the direction of all vectors u of weight $wt(u) = 1$ are balanced functions, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5, \quad \forall u \in V_n, \quad wt(u) = 1. \quad (6)$$

In Table 5 we present the results of research of the values of the algebraic degree of nonlinearity of 4-functions constituted by the component Boolean functions that correspond and do not correspond to the strict avalanche criterion. At the same time, in Table 5, the numbers in curly brackets indicate the probabilities of the formation of 4-function f_4 with a given algebraic degree of nonlinearity when using Boolean functions f_{20} and f_{21}, which (do not) correspond to the strict avalanche criterion.

Table 5
Relationship between the strict avalanche criterion for Boolean functions and the algebraic nonlinearity of 4-functions

Strict avalanche criterion	$\deg(f_4)$
Do not correspond	0 { 10^{-9} }, 1 { $1.59\cdot10^{-8}$ }, 2 { $1.43\cdot10^{-6}$ }, 3 { $3.86\cdot10^{-5}$ }, 4 {0.0142}, 5 {0.2037}, 6 {0.7821}
Correspond	2 { $1.6\cdot10^{-4}$ }, 3 {0.0256}, 4{0.1096}, 5{0.8646}

Analysis of the data presented in Table 5 allows us to conclude that 4-functions of length $N = 16$ based on Boolean functions that correspond to the strict avalanche criterion generally have an algebraic degree of nonlinearity greater than 2 and most likely equal to 5.

3.4. Correlation Immunity of Component Boolean Functions

The correlation immunity of the order m of Boolean function means that its output is not dependent on any group of size m of its input variables.

Since the correlation immunity of order $m > 1$ of the Boolean function is a very strict requirement and is rarely used in practice, we consider the case of correlation-immune of order $m = 1$ Boolean functions.

The determination of the correspondence of the Boolean function to the criterion of correlation immunity is performed on the basis of the following definition.

Definition 2 [15, 16]. A Boolean function $f(x)$, $x \in V_k$, is called correlation-immune of the order m, $1 \le m \le k$, if weight is equal $wt(f') = wt(f)/2^m$, for any of its subfunction f' of $k - m$ variables, while the subfunction of the Boolean function $f(x)$, $x \in V_k$, is a function obtained by substituting into it constants "0" or "1" instead of some of the variables.

In Table 6 we present the results of research on the values of the algebraic degree of nonlinearity of 4-functions constructed on the basis of component Boolean functions that

correspond and do not correspond to the correlation immunity criterion of order $m=1$. In Table 6, the numbers in curly brackets indicate the probabilities of the formation of 4-function f_4 with a given algebraic degree of nonlinearity when using Boolean functions f_{20} and f_{21}, which (do not) correspond to the correlation immunity criterion.

Table 6
Relationship between the correlation immunity of Boolean functions and the algebraic nonlinearity of 4-functions

Correlation immunity of order $m=1$	$\deg(f_4)$
Do not correspond	2 {$1.43\cdot10^{-6}$}, 3 {$1.71\cdot10^{-4}$}, 4 {0.0149}, 5 {0.2298}, 6 {0.7551}
Correspond	0 { $9.53\cdot10^{-6}$}, 1 {$8.57\cdot10^{-5}$}, 2 {0.0013}, 3 {0.0628}, 4 {0.1920}, 5 {0.7438}

Analysis of the data presented in Table 6 allows us to conclude that the largest number of 4-functions that are constituted from the correlation-immune Boolean functions has an algebraic degree of nonlinearity equal to 5.

4. Conclusions

In this paper, research devoted to understanding the relationship between the algebraic degree of nonlinearity of 4-functions of two variables and the cryptographic properties of its component Boolean functions are performed. The obtained results allowing us to form the following conclusions that are significant for the development of cryptographic primitives:

1. A larger algebraic degree of nonlinearity of the component Boolean functions leads to a larger algebraic degree of nonlinearity of a resulting 4-function.
2. Odd values of the nonlinearity distance of the component Boolean functions lead to the formation of a 4-function with the maximum algebraic degree of nonlinearity.
3. 4-functions consisting of component Boolean functions that satisfy the strict avalanche criterion are most likely to have an algebraic degree of nonlinearity equal to 5.
4. 4-functions consisting of component Boolean functions that satisfy the correlation immunity criterion are most likely to have an algebraic degree of nonlinearity equal to 5.
5. there are no 4-functions with algebraic degree of nonlinearity equal to 6 that are constituted from Boolean functions that correspond to strict avalanche criterion or the criterion of correlation immunity.

Of practical interest are further research devoted to identification of more general patterns that reflect the relationship between the criteria for the cryptographic quality of many-valued logic functions of an arbitrary number of variables and their component Boolean functions.

References

[1] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.

[2] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 240–245.

[3] A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

[4] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[5] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves, in: 2nd Int. Workshop on Modern Machine Learning Technologies and Data Science, no. I, vol. 2631 (2020) 30–39.

[6] A. Elhosary et al., State of the Art in Boolean Functions Cryptographic Assessment, Int. J. Comput. Netw. Commun. Secur. (2013) 88–94.
[7] O. Logachev, A. Sal'nikov, V. Jashhenko, Boolean Functions in Coding Theory and Cryptology, Publishing House MCNMO (2004).
[8] A. Sokolov, O. Zhdanov, Cryptographic Constructions Based on Many-Valued Logic Functions, Monograph, Publishing House Scientific Thought (2020).
[9] A. Sokolov, et al., Prerequisites for Developing a Methodology for Estimating and Increasing Cryptographic Strength Based on Many-Valued Logic Functions, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 2923 (2021) 107–116.
[10] A. Rostovcev, Cryptography and Data Protection, Publishing House World and Family (2002).
[11] R. Stanković, J. Astola, C. Moraga, Representations of Multiple-Valued Logic Functions, Morgan&Claypool Publishers (2012).
[12] F. Rodier, On the Nonlinearity of Boolean Functions, WCC2003, Workshop on Coding and Cryptography (2003) 397–405.
[13] R. Forré, The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition, Advances in Cryptology, LNCS 403 (1990) 450–468.
[14] A. Sokolov, Constructive Method for the Synthesis of Nonlinear S-boxes Satisfying the Strict Avalanche Criterion, Radioelectron. Commun. Syst. 56(8) (2013) 415–423. doi: 10.3103/S0735 272713080049.
[15] S. Picek et al., Correlation Immunity of Boolean Functions: An Evolutionary Algorithms Perspective, Annual Conference on Genetic and Evolutionary Computation (2015) 1095–1102. doi: 10.1145/2739480.2754764.
[16] K. Kim, Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC, Advances in Cryptology—ASIACRYPT'91, LNCS 739 (1991) 59–73.