UDC 004.056.55

NYBERG CONSTRUCTION NONLINEAR TRANSFORMS BASED ON ALL ISOMORPHIC REPRESENTATIONS OF THE GALOIS FIELD GF (512)

A.V. SOKOLOV

Odessa National Polytechnic University

Abstract *– The paper deals with questions of increasing the efficiency of block symmetric cryptographic algorithms used in modern telecommunications systems. One of the most important elements of any modern symmetric block cryptographic algorithm is its nonlinear transform or* S *-box, which largely determines its cryptographic features and performance. Therefore the task of development of a large set of cryptographic* S *-boxes with a high level of quality is the key to solving the problem of increasing the efficiency of modern cryptographic algorithms. The basis of one of the most common block symmetric cryptographic algorithms AES/Rijndael is the nonlinear transform of Nyberg design of length* $N = 256$*. This design allows construction of a small set of nonlinear transforms which have a high level of cryptographic quality. However, the development of modern computer technology dictates not only the task of building of* S *-boxes of greater length, as well as finding ways to increase the cardinality of sets of available high quality non-linear transforms. In this paper a class of* S *-boxes of Nyberg design with cardinality* $J = 392$ *and the length* $N = 512$ *over all the isomorphic representations of the field* $GF(512)$ *is built, which allows improvement of the efficiency of cryptographic nonlinear transforms, as well as to increase the cardinality of their sets. The dynamics of improvement of the cryptographic quality of* S *-boxes of Nyberg design with increasing of their length are investigated. It was found that increasing of the length of nonlinear transforms of Nyberg design gives the rapid decline of correlation between vectors of output and input of* S *-box as well as significant growth of its distance of nonlinearity. It is shown that great length* S *-boxes of Nyberg design obtains such distance of nonlinearity, that it becomes almost equivalent to the distance of the nonlinearity of Boolean bent-functions.*

Анотація *– У статті розглянуті питання побудови класу* S *-блоків підстановки конструкції Ніберг потужності* $J = 392$*, довжини* $N = 512$ *над усіма ізоморфними уявленнями поля* $GF(512)$*. Досліджено криптографічну якість побудованих* S *-блоків, а також динаміку її поліпшення із зростанням довжини нелінійного перетворення.*

Аннотация *– В статье рассмотрены вопросы построения класса* S *-блоков подстановки конструкции Ниберг мощности* $J = 392$*, длины* $N = 512$ *над всеми изоморфными представлениями поля* $GF(512)$*. Изучены криптографические качества построенных* S *-блоков, а также динамика их улучшения с ростом длины нелинейного преобразования.*

Construction of any protected modern telecommunication system is linked inextricably to issues of design of cryptographic subsystem of information protection. Since high performance and relatively good cryptographic reliability of block symmetric cryptographic algorithms they are widely used now. One of such popular algorithms is AES/Rijndael, accepted as the sovereign-governmental US standard.

One of the main components of any modern cryptographic algorithm is the nonlinear transform — S-box. Structure and properties of S-box largely determines the properties of the cryptographic algorithm and significantly affects its performance [1].

One of the most successful approaches for solving the problem of synthesis of S-boxes having reasonable level of quality is an approach based on the mathematical apparatus of the theory of Boolean functions. This approach revealed that with increasing of length of S-boxes their cryptographic quality significantly improves, and hence, the effectiveness of cryptographic algorithms in which they are applied.

On the other hand, is a very actual task of building a large plurality of good quality S-boxes, which opens the possibility of using them as a long-term key element, as for example allowed in the standard GOST 28147-89 [2].

As significant progress in solving these two problems became the synthesis method of Nyberg construction S-boxes, which allows the building of highly nonlinear transforms based on the algebraic Galois fields [3]. Further research allowed improvement of this method by considering the extension of an extended Galois field and resulted in significantly expanding the range of available high-quality S-boxes of length $N=256$ [4].

Hence, the further practical interest is the increase in length of S-boxes, whereas the construction methods of nonlinear transforms of length $N>256$ are not sufficiently researched in the literature.

The purpose of this paper is to develop a method of the synthesis of S-boxes of length $N=512$ based on all isomorphic representations of the field $GF(512)$ for encryption tasks in modern telecommunication systems.

The classical Nyberg nonlinear transform is a mapping of a multiplicative inverse elements of the Galois field [3]:

$$y = x^{-1} mod(f(z), p), \quad y, x \in GF(2^k), \tag{1}$$

combined with an affine transformation

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{y} + \mathbf{a}, \quad \mathbf{a}, \mathbf{b} \in GF(2^k), \tag{2}$$

where $f(z)$ is an irreducible polynomial over the field $GF(2)$;

$\mathbf{A}$ — nonsingular affine transformation matrix;

$\mathbf{a}$ — shift vector;

$p=2$ — the characteristic of the extended Galois field, and $0^{-1}=0$;

$\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}$ — elements of the extended Galois field; treated as decimal numbers or binary vectors, or polynomials.

Analysis of (1) leads to the conclusion that the cryptographic properties of S-boxes depends on the choice of the form of an irreducible polynomial $f(z)$, while the affine transformation (2) affects the correlation between output and input of the S-box [5] of Nyberg construction and its periods of return to initial state [6].

It is significant that the Nyberg construction S-box can be implemented as a look-up table, and with the help of an algebraic transformation (1), (2), which determines its flexibility in terms of resource consumption of the memory subsystem.

The total number of available different S-boxes of Nyberg construction is determined by the number of, existing in the field $GF(q^k)$, irreducible polynomials [7]

$$\left|\mathbf{W}_q^k\right| = \frac{1}{k}\sum_{\substack{d \\ d/k}} \mu(d) q^{(k/d)}, \tag{3}$$

where d — divisors of degree k; $\mu(d)$ — Mobius function; notation d/k means that d divides k.

In particular, when $k=9$, i.e. for the field $GF(2^9)=GF(512)$ there $\left|\mathbf{W}_2^9\right|=56$. The set of these polynomials are written for short as their decimal equivalents.

$$\begin{aligned}\mathbf{W}_2^9 = \{&515,529,535,539,545,557,563,587,601,607,613,617,623,631,637,647,\\ &661,665,675,677,687,695,701,719,721,731,757,761,769,787,789,799,\\ &803,817,827,841,847,859,865,875,877,883,895,901,911,929,949,953,\\ &967,971,973,981,985,995,1001,1019\}.\end{aligned} \tag{4}$$

For example, the first decimal equivalent of (4) can be converted into a polynomial form $515_{10} = 1000000011_2 \Rightarrow f_1(z) = z^9 + z + 1$. Clearly, each of the polynomials (4) in accordance with (1) and (2) determine a unique structure of S-box. On the other hand, researches [4] indicate that the number of different structures of S-boxes can be significantly extended by the consideration of all isomorphic representations of the original field $GF(2^9)$. The original field allows the following representations

$$GF(512) = GF(2^9) = GF(8^3). \tag{5}$$

Using (3) to that obtained in (5) expansion, we find that there are $\xi = 168$ more different structures of the irreducible polynomials. However, the extended arithmetic field $GF(8)$ can be constructed in two different ways, determined by the corresponding primitive polynomials

$$\begin{cases}\eta_1(x) = x^3 + x^1 + 1;\\ \eta_2(x) = x^3 + x^2 + 1.\end{cases} \tag{6}$$

Thus, the total number of irreducible polynomials and respectively the various structures of S-boxes in the field $GF(8^3)$ is defined as $\left|\mathbf{W}_8^3\right| = 2 \cdot 168 = 336$.

For example, the set of all irreducible polynomials decimal equivalents in the field $GF(8^3)$ with arithmetic defined by primitive polynomial $\eta_1(x)$ from (6) has the form

$$\begin{aligned}\mathbf{W}_8^3 = \{&522,524,526,529,532,533,539,540,543,545,550,551,555,557,558,561,562,563,\\ &570,573,575,578,580,582,593,597,598,602,606,607,609,610,615,618,619,620,\\ &625,627,628,636,637,638,641,646,647,649,652,655,661,662,663,665,667,668,\\ &683,685,687,690,691,694,697,698,702,707,709,710,714,716,717,721,723,724,\\ &732,734,735,737,739,741,754,757,758,763,766,767,769,770,771,777,779,782,\\ &786,788,789,793,794,796,802,803,807,809,813,814,827,829,831,834,837,839,\\ &844,846,847,850,852,855,858,859,861,865,869,870,874,875,878,881,885,887,\\ &897,900,901,905,906,909,923,925,927,932,934,935,937,940,942,947,948,949,\\ &953,954,959,963,964,967,970,971,974,977,979,983,995,996,998,1004,1005,\\ &1007,1009,1010,1015,1018,1020,1021\}.\end{aligned} \tag{7}$$

and, accordingly, the set of decimal equivalents of irreducible polynomials constructed above with the arithmetic defined by primitive polynomial $\eta_2(x)$ from (6)

$$\begin{aligned}\mathbf{W}_8^3 = \{&523,525,526,530,533,535,537,540,541,546,548,550,553,558,559,561,562,563,\\ &571,572,575,579,581,582,595,598,599,601,604,606,610,611,613,617,619,623,\\ &625,626,629,636,637,638,642,644,646,651,652,653,661,662,663,665,666,669,\\ &681,682,684,691,692,694,698,702,703,705,710,711,713,717,719,721,722,725,\\ &732,734,735,738,740,743,754,755,758,761,763,766,771,772,775,781,782,783,\\ &786,787,788,795,797,799,802,803,806,809,812,814,817,820,823,833,834,835,\\ &841,842,846,849,851,853,859,860,861,865,868,870,874,875,879,890,892,895,\\ &897,900,901,905,907,908,914,916,919,929,933,934,941,942,943,946,948,949,\\ &953,955,959,962,965,967,970,971,974,985,986,991,996,997,999,1002,1005,\\ &1006,1009,1011,1015,1019,1020,1021\}.\end{aligned} \tag{8}$$

Consider the polynomial 523 from (8), which can be represented by a polynomial-form as $523_{10} = 1013_8 = x^3 + x + 3$, based on which and in accordance with (1) the Nyberg construction S-box can be built

$$S=\left\{\begin{array}{c}
0,1,6,4,3,7,2,5,200,109,138,470,192,436,398,442,496,243,420,233,113,448,331,\\
218,96,64,151,283,181,426,357,162,344,311,479,505,210,414,486,320,312,339,157,\\
256,381,457,366,251,400,276,384,81,77,92,191,225,168,291,271,495,124,300,128,\\
374,25,97,392,335,506,488,459,89,165,158,143,372,93,52,348,454,385,51,307,239,\\
144,315,104,493,458,71,126,205,53,76,245,410,24,65,140,237,209,299,364,228,86,\\
492,453,424,201,9,362,480,449,20,172,463,445,148,474,227,423,252,322,146,60,\\
301,90,204,62,375,406,446,240,361,309,352,326,377,10,471,98,236,373,74,84,314,\\
123,323,117,444,282,26,213,441,490,498,257,42,73,164,198,416,31,356,159,72,485,\\
175,56,290,390,466,114,462,484,167,369,476,389,249,427,28,500,434,395,289,354,\\
336,324,502,224,54,12,437,408,316,268,230,160,417,8,108,473,260,127,91,359,\\
223,298,100,36,415,440,152,387,221,379,267,23,330,386,215,358,207,190,55,475,\\
119,103,365,197,269,421,19,295,262,141,99,306,83,132,360,497,17,411,94,465,280,\\
388,179,367,47,121,422,351,397,43,156,285,272,203,472,235,294,286,346,378,217,\\
196,231,494,58,259,284,302,433,49,401,333,482,247,464,150,27,273,258,264,347,\\
394,185,169,57,431,412,263,234,451,340,208,101,61,125,274,432,460,438,238,82,\\
353,134,345,33,40,338,145,85,195,409,329,371,39,487,122,147,188,503,136,376,\\
370,318,219,22,483,278,393,67,187,355,313,41,297,450,510,469,32,310,265,287,78,\\
455,396,254,135,308,186,337,163,30,222,206,241,133,110,481,102,229,46,250,477,\\
176,328,319,75,142,63,129,327,137,266,216,456,44,404,428,50,80,220,214,248,178,\\
170,467,66,334,288,184,350,255,14,443,48,277,418,509,382,429,130,447,194,317,\\
95,244,293,430,37,211,161,199,402,508,18,232,253,120,107,452,29,180,383,405,413,\\
292,303,275,183,501,13,193,305,461,212,153,15,399,149,116,131,407,21,112,341,\\
296,425,106,79,349,380,45,88,70,304,439,173,115,281,246,171,391,511,343,11,139,\\
261,202,118,226,177,368,504,34,111,363,279,332,174,166,38,321,69,507,154,499,\\
105,87,270,59,16,242,155,491,182,435,189,325,478,35,68,489,419,403,342,468
\end{array}\right\}. \qquad (9)$$

Consider in more detail the cryptographic quality of S-box (9). Thus, this S-box can be decomposed into $k=9$ component Boolean functions

$$S=\{F_1;F_2;F_3;F_4;F_5;F_6;F_7;F_8;F_9\}, \qquad (10)$$

algebraic degree of nonlinearity [5] of each of which is $\mathbf{deg}(F_i)=8$, $i=1,2,...,9$.

For each of component Boolean functions (10) can be calculated the distance of the nonlinearity as the minimum distance from the component Boolean functions F_i to the set of affine functions A_j [8]

$$N_s=\mathbf{min}\{N_f\}=\mathbf{min}\{dist(F_i,A_j)\}, \quad i=1,2,...,k, \quad j=1,2,...,2^{k+1}. \qquad (11)$$

It is easy to calculate that, for S-box (9), the distance of nonlinearity (11) is equal to the $N_s=234$.

Fig. 1 shows the change of the distance of nonlinearity dependent on the growth of length $N = 2^k$ of the Nyberg construction S-box compared with the growth of distance of nonlinearity of the most nonlinear algebraic structures — bent-functions.

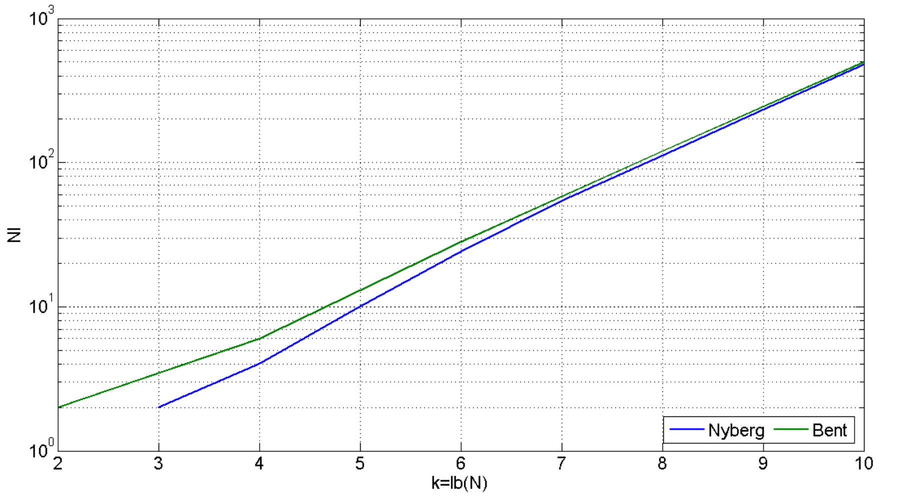

Fig. 1. The dependence of the nonlinearity of component Boolean functions of Nyberg construction S-boxes and bent-functions from their length

The analysis of Fig. 1 shows very high nonlinear quality of S-boxes of Nyberg construction, actually approaching the nonlinearity of bent-functions.

Another important criterion is the matrix $R = \left\| r_{i,j} \right\|$, $i, j = 0,1,\ldots,k-1$ of correlation coefficients of the output and input of S-box, defined as:

$$r_{i,j} = 1 - 2^{-(k-1)} \sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j}), \quad i, j = 0,1,\ldots,k-1. \tag{12}$$

For S-box (9) the matrix of correlation coefficients (12) of output and input is:

$$R = \begin{pmatrix} 0.008 & 0.008 & 0.008 & -0.063 & 0.07 & 0.055 & 0.07 & 0.039 & 0.055 \\ 0.008 & 0.078 & 0.008 & 0.07 & -0.023 & -0.063 & 0.039 & 0.063 & 0.07 \\ 0.008 & 0.008 & 0.031 & 0.055 & -0.063 & 0.063 & 0.055 & 0.07 & -0.016 \\ -0.063 & 0.07 & 0.055 & -0.031 & -0.047 & -0.031 & 0.078 & -0.063 & 0.008 \\ 0.07 & -0.023 & -0.063 & -0.047 & 0.031 & -0.031 & -0.063 & 0.055 & 0.078 \\ 0.055 & -0.063 & 0.063 & -0.031 & -0.031 & -0.016 & 0.008 & 0.078 & 0.008 \\ 0.07 & 0.039 & 0.055 & 0.078 & -0.063 & 0.008 & 0.016 & -0.016 & -0.047 \\ 0.039 & 0.063 & 0.07 & -0.063 & 0.055 & 0.078 & -0.016 & -0.031 & 0.016 \\ 0.055 & 0.07 & -0.016 & 0.008 & 0.078 & 0.008 & -0.047 & 0.016 & -0.031 \end{pmatrix}. \tag{13}$$

Note that the maximum correlation coefficient of matrix (13) is equal to $\mathbf{max}\{R\} = 0.0781$. The number of zeros in the matrix of correlation coefficients is $K^0 = 0$.

Fig. 2 shows the dependence of the fall of correlation interconnection between output and input of Nyberg construction S-boxes with increase in their length.

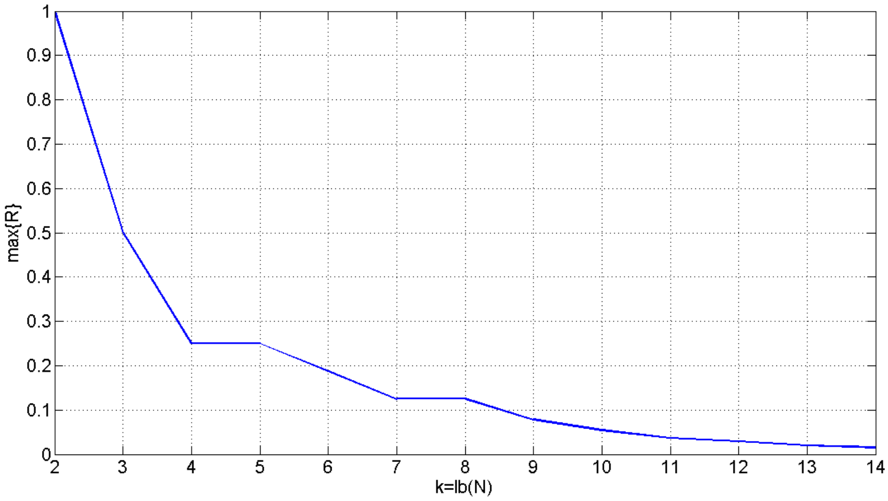

Fig. 2. The dependence of correlation of output and input of Nyberg construction S-boxes from their length

Another important quality criterion of S-boxes are their differential properties, characterized by weight of directional derivatives of component Boolean functions $D_{i,\nu} = F_i(x) \oplus F_i(x \oplus e_\nu)$ in all directions e_ν of weight $wt(e_\nu) = 1$ [9]. For S-box (9) weight matrix of directional derivatives of component Boolean functions is shown in Table 1.

Table 1. Weight matrix of directional derivatives of component Boolean functions of S-box (9)

e_j	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$	$wt\left(D_{9,k}\right)$
100000000	256	236	248	264	248	260	252	264	264
010000000	236	244	256	248	236	264	264	236	252
001000000	244	256	236	236	264	248	236	268	264
000100000	264	248	260	264	260	272	244	256	236
000010000	248	236	264	260	244	264	256	256	244
000001000	236	264	248	244	240	260	256	272	256
000000100	264	260	272	256	256	248	236	264	248
000000010	260	244	264	256	256	256	264	268	236
000000001	244	240	260	256	236	256	268	252	264

The return period to initial state for S-box (9) is equal to $T = 2$.

Table 2 shows the cryptographic properties of S-boxes of Nyberg construction for different representations of the original field $GF(512)$.

Table 2. Cryptographic properties of S-boxes

Galois field	The number of primitives polynomials	$\max\{\|r_{i,j}\|\}$	K^0	N_s	$\min\{\deg(F_i)\}$	T
$GF(2^9)$	56	0.0625…0.0859	0…21	234	8	2
$GF(8^3)$, polynomial $\eta_1(x)$	168	0.0547…0.0859	0…8	234	8	108…29260
$GF(8^3)$, polynomial $\eta_2(x)$	168	0.0547…0.0859	0…9	234	8	48…29260

In conclusion, we note the main results of the research:

1. For the first time Nyberg construction S-boxes of length $N = 512$ are constructed. It is shown that these nonlinear transforms have a high level of cryptographic quality, which allows their recommendation for usage in modern and promising cryptographic algorithms for encryption purposes in telecommunication systems.

2. The complete class of all isomorphic representations of the field $GF(512)$ are considered, which allows a significant increase in the number of high-quality Nyberg construction S-boxes to the power of set $J = 392$. The complete classes of irreducible polynomials for the field $GF(8^3)$ are obtained, which is important from the point of view of practical implementation of the developed S-boxes.

3. The dynamics of nonlinearity changes and correlation properties of Nyberg construction S-boxes with increasing of their length are researched.

References:

1. *Долгов В.И., Олейников Р.В., Лисицкая И.В., Сергиенко Р.В. и др.* Подстановочные конструкции современных симметричных блочных шифров // Радіоелектронні і комп'ютерні системи. – 2009. — № 6. – С. 89-93.

2. Государственный стандарт Союза ССР. Системы обработки информации. Криптографическая защита. Алгоритм криптографического преобразования ГОСТ 28147–89. – М.: ИПК Издательство Стандартов, 1990. – 28 с.

3. *Nyberg K.* Differentially uniform mappings for cryptography // Advances in cryptology Advances in Cryptology — EUROCRYPT '93. Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993. — Springer Berlin Heidelberg, 1994. — P. 55-65.

4. *Mazurkov M.I., Sokolov A.V.* Non-linear S-box of Nyberg construction with maximal avalanche effect // Radioelectronics and Communications Systems. — 2014. — Vol. 57, No 6. — P. 274-281.

5. *Соколов А.В.* Новые методы синтеза нелинейных преобразований современных шифров. — Lap Lambert Academic Publishing, 2015. – 100 с.

6. *Зайко Ю.Н.* Криптография глазами физика // Изв. Саратовского ун-та. – 2009.— Т. 9, Вып. 2. – С. 34-48.

7. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971. – 477 с.

8. *Maier W., Staffelbach O.* Nonlinearity criteria for cryptographic functions // In Advances in Cryptology — EUROCRYPT'89. Workshop on the Theory and Application of Cryptographic Techniques Houthalen, Belgium, April 10–13, 1989. – Springer Berlin Heidelberg, 1990. — P. 549-562.

9. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: Издательство МЦНМО, 2004. – 472 с.