Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions

Artem Sokolov [0000-0003-0283-7229] and Djiofack Temgoua Vanissa Noel [0000-0003-1651-0702]

Odessa National Polytechnic University, Odessa, Ukraine
radiosquid@gmail.com

Abstract. S-boxes of the Nyberg construction are one of the most important cryptographic primitives, which are used in the AES cryptographic algorithm and largely determines its effectiveness. Numerous researches have confirmed the high cryptographic quality of their component Boolean functions. Nevertheless, the cryptanalyst is not constrained in the methods used and can also use the mathematical apparatus of the functions of many-valued logic for cryptanalysis. This work is devoted to the research of the nonlinear properties of S-boxes of the Nyberg construction, presented in the form of component 4-functions and 16-functions. The paper proposes a method for calculating the nonlinearity value of 16-functions, for which the formula of the recursive construction of hexadecimal Vilenkin-Chrestenson matrices of arbitrary order is discovered. The performed researches made it possible to establish that the nonlinearity values of component 4-functions and 16-functions of S-boxes of the Nyberg construction is not stable and depends on the type of irreducible polynomial used to construct them. In the paper we present the irreducible polynomial for which the nonlinearity values of component 4-functions and 16-functions is evenly high. At the same time, it was established that the same polynomial also provides the uniform minimization of the correlation coefficients between output and input vectors of the S-box. The specified polynomial can be recommended for the practical use.

Keywords: cryptography, logic, function, Nyberg construction, nonlinearity, S-box.

1 Introduction and problem statement

Block symmetric cryptographic algorithms are a very important component of modern information security systems. The main component of block symmetric cryptographic algorithms, on which the overall quality of the cryptographic transform depends, is a cryptographic S-box. Today, there are many constructive methods for the synthesis of high-quality S-boxes. As one of the most effective methods for S-boxes design the Nyberg construction can be mentioned [1]. S-boxes of this construction are used in the Rijndael cryptographic algorithm, which is approved as the AES encryption standard [2].

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

S-boxes of the Nyberg construction are determined by using a mapping in the form of multiplicatively inverse elements of the Galois field $GF(2^k)$

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

which is in general combined with an affine transform

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

where as $f(z)$ the standard AES irreducible over the field $GF(2)$ polynomial is used $f(z) = z^8 + z^4 + z^3 + z + 1$;

A is the nonsingular affine transform matrix;

a is the shift vector;

$p = 2$ is the characteristic of the extended Galois field, $0^{-1} \equiv 0$ is taken a-priory;

a, b, x, y are the elements of the extended Galois field, that can be considered as decimal numbers, or binary vectors, or polynomials of degree $k-1$.

A detailed research of the cryptographic properties of Nyberg construction S-boxes of length $N = 256$ was performed in [3], where it was established that the crypto-graphic quality of the S-box depends on the type of irreducible polynomial used. The number of irreducible polynomials is defined as

$$|W_k| = \frac{1}{k} \sum_{\substack{d \\ d \ \ k}} \mu(d) \cdot p^{(k/d)}, \tag{3}$$

where d are the divisors of the k, $\mu(d)$ is the Mobius function, the notation $d \quad k$ means that d divides k.

Moreover, to determine the cryptographic quality of S-boxes, the generally accept-ed approach is to represent the S-box using the mathematical apparatus of Boolean algebra: the original S-box is decomposed into component Boolean functions, to each of which a generally accepted set of criteria for cryptographic quality is used. In this set of criteria, the criterion of high nonlinearity is adopted as the most important crite-rion [4].

Nevertheless, when describing cryptographic algorithms, a cryptanalyst is not con-strained in the facilities used, in particular, the mathematical apparatus of functions of many-valued logic can be used [5]. Today in the literature there are no researches of the nonlinear properties of S-boxes of the Nyberg construction, presented using the functions of many-valued logic.

The *purpose* of this work is to research the nonlinear properties of the component many-valued logic functions of Nyberg construction S-boxes of length $N = 256$ based on the full set of irreducible polynomials.

2 Possible representations of AES S-boxes by functions of many-valued logic

We introduce the definition of the S-box which is necessary for further research and consider the possible forms of its representation.

Definition 1. S-box is a substitution of the form

$$\begin{pmatrix} 0 & \cdots & N-1 \\ y_0 & \cdots & y_{N-1} \end{pmatrix}, \tag{4}$$

where the first row is a sequence of numbers from 0 to $N-1$, the second row is a sequence $\{y_i\}$ consisting of elements of the first row, rearranged according to the law specified by the designers of the S-box. The second row of the substitution (4) is called as the coding Q-sequence and denoted $Q=\{y_i\}$, $i=0,1,...,N-1$.

Each coding Q-sequence can be unambiguously represented in the form of $k=\log_q N$ its component q-functions, where q belongs to the set of such values that the length N of the S-box can be represented in the form $N=q^k$.

Obviously, the Nyberg S-boxes used in the AES cryptoalgorithm can be uniquely represented using component Boolean functions (2-functions), using component 4-functions, and also using component 16-functions. Moreover, each of these functions completely determines the structure and cryptographic quality of the S-box in the sense of the corresponding logic.

For example, consider the S-box of the Nyberg construction (1) based on a polynomial $f(z)=283_{10}=z^8+z^4+z^3+z+1$ used in the AES cipher in the form of its coding Q-sequence

Q={0 1 141 246 203 82 123 209 232 79 41 192 176 225 229 199
116 180 170 75 153 43 96 95 88 63 253 204 255 64 238 178 58
110 90 241 85 77 168 201 193 10 152 21 48 68 162 194 44 69
146 108 243 57 102 66 242 53 32 111 119 187 89 25 29 254 55
103 45 49 245 105 167 100 171 19 84 37 233 9 237 92 5 202
76 36 135 191 24 62 34 240 81 236 97 23 22 94 175 211 73
166 54 67 244 71 145 223 51 147 33 59 121 183 151 133 16 181
186 60 182 112 208 6 161 250 129 130 131 126 127 128 150 115
190 86 155 158 149 217 247 2 185 164 222 106 50 109 216 138 (5)
132 114 42 20 159 136 249 220 137 154 251 124 46 195 143 184
101 72 38 200 18 74 206 231 210 98 12 224 31 239 17 117 120
113 165 142 118 61 189 188 134 87 11 40 47 163 218 212 228 15
169 39 83 4 27 252 172 230 122 7 174 99 197 219 226 234 148
139 196 213 157 248 144 107 177 13 214 235 198 14 207 173 8 78
215 227 93 80 30 179 91 35 56 52 104 70 3 140 221 156 125
160 205 26 65 28}.

We consider the possible representations of the S-box (5) using the functions of many-valued logic, bringing as an example the first of the corresponding component q-functions. So, the S-box (5) can be represented as 8 component Boolean functions, the first of which is given as an example

$$\begin{array}{c} Fbin_1 = \{01101011011001110001110101101000000111011001000000 \\ 10011000101111110111111101101111010001100001011001110010 \\ 11111111111010000000101010100100101110100001000000001010101 \\ 0011010000000100001111011001100110110001111010000010111000 \\ 1011001110100110011100111000010101010 10\}. \end{array} \tag{6}$$

The S-box (5) can also be represented as four component 4-functions $Ffour_i$, $i = 1, 2, ..., 4$, the first of which has the form

$$\begin{array}{c} Ffour_1 = \{011232310310011300231303031030222221110112010022 0 \\ 120312221033311123311113033011110120033022010132233122303 \\ 133313133101202002121232302322321132102221020220301012302 \\ 330102022232200331101122110233033200313303002232313220301 \\ 10031123222310233102333000230101012 10\}. \end{array} \tag{7}$$

And also, the S-box (5) can be represented as two component 16-functions, the first of which we give as an example

$$\begin{array}{c} Fhex_1 = \{01D6B2B18F90015744AB9B0F8FDCF0E2AEA15D891A85 \\ 0422C52C3962250F7B99DE77D15974B34599DC5AC47F8E201C17 \\ 6EF39663471F331B977505AC60061A123EF063E6BE597294EA2D8 \\ A42A4F89C9ABCE3F858682AE722C0FF15815E6DDC67B8F3A44F \\ 9734BCC6A7E35B2A4B45D80B1D6B6EFD8E73D0E3B384863CDC \\ D0DA1C\}. \end{array} \tag{8}$$

3 Method for determining the nonlinearity value of many-valued logic functions

The most important characteristic of the cryptographic quality of S-boxes is its non-linearity distance. The binary case is classical, in which the nonlinearity distance is defined as the minimum Hamming distance between Boolean function f and all codewords of an affine code [6]

$$2N_f = \min(dist(f, \mathfrak{A}_j)), \quad j = 0, 1, ..., 2^{k+1} - 1. \tag{9}$$

Definition 2. For an arbitrary positive integer k, an affine code $\mathfrak{A}(N, k)$ of length $N = 2^k$ is defined as the set of all rows of those Boolean functions whose algebraic degree of nonlinearity does not exceed 1, that is $\mathfrak{A}(N, k) = \left\{ \mathfrak{A}_f \mid f \in F_k, \deg f \leq 1 \right\}$ [7].

In turn, the nonlinearity distance of the entire S-box is determined by the worst from its component Boolean functions, i.e. as

$$2N_S = \min\{2N_{F_i}\}, \quad i = 1, 2, ..., k_2. \tag{10}$$

Moreover, since the set of codewords of the non-inverse part of the affine code co-incides with the rows of the Walsh-Hadamard matrix, the nonlinearity distance of the component Boolean functions can also be found in the domain of the Walsh-Hadamard transform coefficients in accordance with the following formula

$$2N_f = 2^{k-1} - \frac{1}{2}\max_{v\in Z_2^k}\left|W_f(v)\right|, \tag{11}$$

where $W_f(v) = f \cdot A_N$ is the vector of coefficients of the Walsh-Hadamard transform of the component Boolean function f, A_N is the Walsh-Hadamard matrix, which is constructed in accordance with the following recurrence rule

$$A_{2^{k+1}} = \begin{bmatrix} A_{2^k} & A_{2^k} \\ A_{2^k} & -A_{2^k} \end{bmatrix}, \tag{12}$$

where $A_1 = 1$.

Applying formulas (9) or (11) to the first component Boolean function (6) of the S-box (5), it is easy to verify that its nonlinearity distance is equal to $N_{Fbin_1} = 112$, while the nonlinearity distances of all component Boolean functions of the S-box (5) are equal to $N_{Fbin_i} = \{112,112,112,112,112,112,112,112\}, \quad i = 1,2,...,8$.

Nevertheless, formulas (9) and (11) are not applicable for the estimation of the nonlinearity value of functions of many-valued logic, in particular, for the 4-functions and 16-functions that we are researching.

Estimation of the nonlinearity value of 4-functions is an important problem, which was solved in [8, 11]. The proposed method for estimating the nonlinearity value of 4-functions is based on finding the coefficients of the Vilenkin-Chrestenson transform $\Omega_f = f\overline{V}$ of the investigated 4-function f, where the investigated 4-function f and the Vilenkin-Chrestenson matrix V are presented in exponential form using the unique transformation

$$\{0,1,2,3\} \to \left\{ e^{j\frac{2\pi}{4}\cdot 0} \quad e^{j\frac{2\pi}{4}\cdot 1} \quad e^{j\frac{2\pi}{4}\cdot 2} \quad e^{j\frac{2\pi}{4}\cdot 3} \right\}. \tag{13}$$

The Vilenkin-Chrestenson matrix is constructed according to the following recurrence rule

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \tag{14}$$

where the summation is performed modulo 4, and

$$V_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 3 & 2 & 1 \end{bmatrix}. \quad (15)$$

Based on the Vilenkin-Chrestenson transform coefficients, a generalized formula for estimation of the nonlinearity value of q-valued logic functions is introduced in [8]

$$qN_f = \begin{cases} q^k - \max\left\{\left|\Omega_f\right|\right\}, & q > 2; \\ 2^{k-1} - \frac{1}{2}\max\left\{\left|W_f\right|\right\}, & q = 2. \end{cases} \quad (16)$$

Same to the binary case, the nonlinearity value of the S-box is determined by its worst component q-function, respectively, $qN_S = \min\{qN_{F_i}\}, \quad i = 1, 2, ..., k_q$.

Using expression (14), it is easy to construct the Vilenkin-Chrestenson matrix over the alphabet $\{0,1,2,3\}$ of order $N = 256$, with help of which we can find the coefficients of the Vilenkin-Chrestenson transform of sequence (7). Further, using expression (16), it is not difficult to determine that the nonlinearity value of the 4-function (7) is equal to $4N_{F_1} = 219.5034$. The nonlinearity value of the remaining component 4-functions are equal to $4N_{Ffour_i} = \{219.5034 \;\; 221.9412 \;\; 216.5538 \;\; 219.2849\}$, $i = 1, 2, 3, 4$. Accordingly, the nonlinearity value of the entire S-box (5) is equal to $4N_S = 216.5538$. Note that, in contrast to the binary case, the nonlinearity values of the component 4-functions of S-boxes of the Nyberg construction are different for different component 4-functions [12-13].

Although the general formula for the nonlinearity value for an arbitrary q was introduced in [8], however, a specific mechanism for finding the nonlinearity value of 16-functions was not shown, and in order to evaluate the nonlinearity values of the component 16-functions of the Nyberg construction S-boxes, it is necessary to develop recurrence algorithm for constructing Vilenkin-Chrestenson matrices over the alphabet

$$\left\{ \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ e^{j\frac{2\pi}{16}\cdot 0} & e^{j\frac{2\pi}{16}\cdot 1} & e^{j\frac{2\pi}{16}\cdot 2} & e^{j\frac{2\pi}{16}\cdot 3} & e^{j\frac{2\pi}{16}\cdot 4} & e^{j\frac{2\pi}{16}\cdot 5} & e^{j\frac{2\pi}{16}\cdot 6} & e^{j\frac{2\pi}{16}\cdot 7} \\ 8 & 9 & A & B & C & D & E & F \\ e^{j\frac{2\pi}{16}\cdot 8} & e^{j\frac{2\pi}{16}\cdot 9} & e^{j\frac{2\pi}{16}\cdot 10} & e^{j\frac{2\pi}{16}\cdot 11} & e^{j\frac{2\pi}{16}\cdot 12} & e^{j\frac{2\pi}{16}\cdot 13} & e^{j\frac{2\pi}{16}\cdot 14} & e^{j\frac{2\pi}{16}\cdot 15} \end{matrix} \right\}. \quad (17)$$

Obviously, the affine functions of a $k = 1$ variable over the alphabet (17) have a general form $\varphi_i(x_1) = a_1 x_1 + a_0$. Taking $a_0 = 0$, we construct 16 affine 16-functions $\varphi_1, ..., \varphi_{16}$

$$
\begin{array}{r|c}
\varphi_1 = 0 & 0000000000000000 \\
\varphi_2 = x_1 & 0123456789ABCDEF \\
\varphi_3 = 2x_1 & 02468ACE02468ACE \\
\varphi_4 = 3x_1 & 0369CF258BE147AD \\
\varphi_5 = 4x_1 & 048C048C048C048C \\
\varphi_6 = 5x_1 & 05AF49E38D27C16B \\
\varphi_7 = 6x_1 & 06C28E4A06C28E4A \\
\varphi_8 = 7x_1 & 07E5C3A18F6D4B29 \\
\varphi_9 = 8x_1 & 0808080808080808 \\
\varphi_{10} = 9x_1 & 092B4D6F81A3C5E7 \\
\varphi_{11} = Ax_1 & 0A4E82C60A4E82C6 \\
\varphi_{12} = Bx_1 & 0B61C72D83E94FA5 \\
\varphi_{13} = Cx_1 & 0C840C840C840C84 \\
\varphi_{14} = Dx_1 & 0DA741EB852FC963 \\
\varphi_{15} = Ex_1 & 0ECA86420ECA8642 \\
\varphi_{16} = Dx_1 & 0FEDCBA987654321
\end{array} . \qquad (18)
$$

The resulting set of the first 16 affine 16-functions (18) determines the Vilenkin-Chrestenson matrix of order $N = 16$

$$
V_{16} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\
0&1&2&3&4&5&6&7&8&9&A&B&C&D&E&F \\
0&2&4&6&8&A&C&E&0&2&4&6&8&A&C&E \\
0&3&6&9&C&F&2&5&8&B&E&1&4&7&A&D \\
0&4&8&C&0&4&8&C&0&4&8&C&0&4&8&C \\
0&5&A&F&4&9&E&3&8&D&2&7&C&1&6&B \\
0&6&C&2&8&E&4&A&0&6&C&2&8&E&4&A \\
0&7&E&5&C&3&A&1&8&F&6&D&4&B&2&9 \\
0&8&0&8&0&8&0&8&0&8&0&8&0&8&0&8 \\
0&9&2&B&4&D&6&F&8&1&A&3&C&5&E&7 \\
0&A&4&E&8&2&C&6&0&A&4&E&8&2&C&6 \\
0&B&6&1&C&7&2&D&8&3&E&9&4&F&A&5 \\
0&C&8&4&0&C&8&4&0&C&8&4&0&C&8&4 \\
0&D&A&7&4&1&E&B&8&5&2&F&C&9&6&3 \\
0&E&C&A&8&6&4&2&0&E&C&A&8&6&4&2 \\
0&F&E&D&C&B&A&9&8&7&6&5&4&3&2&1
\end{bmatrix} . \qquad (19)
$$

In view of the fact that for our purposes of researching the nonlinearity values of component 16-functions of S-boxes of the Nyberg construction of length $N = 256$, we need a Vilenkin-Chrestenson matrix of order $N = 256$. Note that the previously used method [9] for constructing Vilenkin-Chrestenson matrices for arbitrary q is complex. It makes the task of developing of simple method for the synthesis of Vilenkin-Chrestenson matrices over the alphabet (17) actual. Researches allowed us to derive a formula for the recurrence construction of Vilenkin-Chrestenson matrices of any given order $N = 16^k$

$$
V_{16^i} = \left[\begin{matrix}
V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} \\
V_{16^i} & V_{16^i}+1 & V_{16^i}+2 & V_{16^i}+3 & V_{16^i}+4 & V_{16^i}+5 & V_{16^i}+6 & V_{16^i}+7 \\
V_{16^i} & V_{16^i}+2 & V_{16^i}+4 & V_{16^i}+6 & V_{16^i}+8 & V_{16^i}+10 & V_{16^i}+12 & V_{16^i}+14 \\
V_{16^i} & V_{16^i}+3 & V_{16^i}+6 & V_{16^i}+9 & V_{16^i}+12 & V_{16^i}+15 & V_{16^i}+2 & V_{16^i}+5 \\
V_{16^i} & V_{16^i}+4 & V_{16^i}+8 & V_{16^i}+12 & V_{16^i} & V_{16^i}+4 & V_{16^i}+8 & V_{16^i}+12 \\
V_{16^i} & V_{16^i}+5 & V_{16^i}+10 & V_{16^i}+15 & V_{16^i}+4 & V_{16^i}+9 & V_{16^i}+14 & V_{16^i}+3 \\
V_{16^i} & V_{16^i}+6 & V_{16^i}+12 & V_{16^i}+2 & V_{16^i}+8 & V_{16^i}+14 & V_{16^i}+4 & V_{16^i}+10 \\
V_{16^i} & V_{16^i}+7 & V_{16^i}+14 & V_{16^i}+5 & V_{16^i}+12 & V_{16^i}+3 & V_{16^i}+10 & V_{16^i}+1 \\
V_{16^i} & V_{16^i}+8 & V_{16^i} & V_{16^i}+8 & V_{16^i} & V_{16^i}+8 & V_{16^i} & V_{16^i}+8 \\
V_{16^i} & V_{16^i}+9 & V_{16^i}+2 & V_{16^i}+11 & V_{16^i}+4 & V_{16^i}+13 & V_{16^i}+6 & V_{16^i}+15 \\
V_{16^i} & V_{16^i}+10 & V_{16^i}+4 & V_{16^i}+14 & V_{16^i}+8 & V_{16^i}+2 & V_{16^i}+12 & V_{16^i}+6 \\
V_{16^i} & V_{16^i}+11 & V_{16^i}+6 & V_{16^i}+1 & V_{16^i}+12 & V_{16^i}+7 & V_{16^i}+2 & V_{16^i}+13 \\
V_{16^i} & V_{16^i}+12 & V_{16^i}+8 & V_{16^i}+4 & V_{16^i} & V_{16^i}+12 & V_{16^i}+8 & V_{16^i}+4 \\
V_{16^i} & V_{16^i}+13 & V_{16^i}+10 & V_{16^i}+7 & V_{16^i}+4 & V_{16^i}+1 & V_{16^i}+14 & V_{16^i}+11 \\
V_{16^i} & V_{16^i}+14 & V_{16^i}+12 & V_{16^i}+10 & V_{16^i}+8 & V_{16^i}+6 & V_{16^i}+4 & V_{16^i}+2 \\
V_{16^i} & V_{16^i}+15 & V_{16^i}+14 & V_{16^i}+13 & V_{16^i}+12 & V_{16^i}+11 & V_{16^i}+10 & V_{16^i}+9
\end{matrix}\right. \tag{20}
$$

$$
\left.\begin{matrix}
V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} & V_{16^i} \\
V_{16^i}+8 & V_{16^i}+9 & V_{16^i}+10 & V_{16^i}+11 & V_{16^i}+12 & V_{16^i}+13 & V_{16^i}+14 & V_{16^i}+15 \\
V_{16^i} & V_{16^i}+2 & V_{16^i}+4 & V_{16^i}+6 & V_{16^i}+8 & V_{16^i}+10 & V_{16^i}+12 & V_{16^i}+14 \\
V_{16^i}+8 & V_{16^i}+11 & V_{16^i}+14 & V_{16^i}+1 & V_{16^i}+4 & V_{16^i}+7 & V_{16^i}+10 & V_{16^i}+13 \\
V_{16^i} & V_{16^i}+4 & V_{16^i}+8 & V_{16^i}+12 & V_{16^i} & V_{16^i}+4 & V_{16^i}+8 & V_{16^i}+12 \\
V_{16^i}+8 & V_{16^i}+13 & V_{16^i}+2 & V_{16^i}+7 & V_{16^i}+12 & V_{16^i}+1 & V_{16^i}+6 & V_{16^i}+11 \\
V_{16^i} & V_{16^i}+6 & V_{16^i}+12 & V_{16^i}+2 & V_{16^i}+8 & V_{16^i}+14 & V_{16^i}+4 & V_{16^i}+10 \\
V_{16^i}+8 & V_{16^i}+15 & V_{16^i}+6 & V_{16^i}+13 & V_{16^i}+4 & V_{16^i}+11 & V_{16^i}+2 & V_{16^i}+9 \\
V_{16^i} & V_{16^i}+8 & V_{16^i} & V_{16^i}+8 & V_{16^i} & V_{16^i}+8 & V_{16^i} & V_{16^i}+8 \\
V_{16^i}+8 & V_{16^i}+1 & V_{16^i}+10 & V_{16^i}+3 & V_{16^i}+12 & V_{16^i}+5 & V_{16^i}+14 & V_{16^i}+7 \\
V_{16^i} & V_{16^i}+10 & V_{16^i}+4 & V_{16^i}+14 & V_{16^i}+8 & V_{16^i}+2 & V_{16^i}+12 & V_{16^i}+6 \\
V_{16^i}+8 & V_{16^i}+3 & V_{16^i}+14 & V_{16^i}+9 & V_{16^i}+4 & V_{16^i}+15 & V_{16^i}+10 & V_{16^i}+5 \\
V_{16^i} & V_{16^i}+12 & V_{16^i}+8 & V_{16^i}+4 & V_{16^i} & V_{16^i}+12 & V_{16^i}+8 & V_{16^i}+4 \\
V_{16^i}+8 & V_{16^i}+5 & V_{16^i}+2 & V_{16^i}+15 & V_{16^i}+12 & V_{16^i}+9 & V_{16^i}+6 & V_{16^i}+3 \\
V_{16^i} & V_{16^i}+14 & V_{16^i}+12 & V_{16^i}+10 & V_{16^i}+8 & V_{16^i}+6 & V_{16^i}+4 & V_{16^i}+2 \\
V_{16^i}+8 & V_{16^i}+7 & V_{16^i}+6 & V_{16^i}+5 & V_{16^i}+4 & V_{16^i}+3 & V_{16^i}+2 & V_{16^i}+1
\end{matrix}\right].
$$

By constructing the Vilenkin-Chrestenson matrix with the help of (20), and also multiplying it by the component 16-function (8) of the S-box (5), it is easy to obtain the Vilenkin-Chrestenson transform coefficients of the 16-function (8). Further, applying formula (16), we find that the nonlinearity value of the 16-function (8) is equal to $16N_{Fhex_1} = 213.8184$. Moreover, the nonlinearity value of the second component 16-function is equal to $16N_{Fhex_2} = 212.4385$, and, accordingly, the nonlinearity value of the entire S-box is equal to $16N_S = 212.4385$.

4 Research of the Nyberg construction S-boxes of length *N*=256 based on the full class of irreducible polynomials

To compare nonlinearity values, it is convenient to use such perfect algebraic constructions as bent-functions [10], which have the minimum possible value of the maximal Vilenkin-Chrestenson transform coefficient equal to $q^{k/2}$, and, accordingly, the maximum nonlinearity value equal to

$$qN_f = q^k - q^{k/2}. \tag{21}$$

Thus, in our case for $q = 4$ and $k = 4$ the maximum value of nonlinearity is equal to $4N_f = 240$, while for $q = 16$ and $k = 2$ the maximum value of nonlinearity will also reach the value $16N_f = 240$.

Using the proposed method for estimating 2-nonlinearity, 4-nonlinearity and 16-nonlinearity values of S-boxes of Nyberg construction of length $N = 256$, it is not difficult to estimate the nonlinearity values for all S-boxes that can be built over a field $GF(256)$. These values are summarized in Table 1.

Table 1. The values of nonlinearity for Nyberg construction S-boxes of length *N*=256.

No.	Irreducible polynomial	$2N_S$	$4N_S$	$16N_S$
1	283	112	216.5538	212.4385
2	285	112	217.7901	208.0271
3	299	112	213.4794	215.6620
4	301	112	212.9187	211.2972
5	313	112	215.7508	213.2651
6	319	112	211.2786	213.6862
7	333	112	215.5031	215.3282
8	351	112	213.4794	219.9423
9	355	112	212.9187	216.2035
10	357	112	217.5292	219.6070
11	361	112	211.8186	215.3785
12	369	112	216.3011	212.2766
13	375	112	219.1218	213.1083
14	379	112	219.1218	200.4
15	391	112	216	214.2562
16	395	112	214.7689	220.3838
17	397	112	215.5031	217.4026
18	415	112	210.6569	202.9546
19	419	112	221.4746	215.3345
20	425	112	215.9500	213.2825
21	433	112	219.7785	217.0560
22	445	112	215.7508	218.4184
23	451	112	217.3736	218.5131
24	463	112	213.6208	211.3523

25	471	112	211.2786	218.9588
26	477	112	217.9474	209.9110
27	487	112	217.5292	207.0381
28	499	112	218.4234	219.6522
29	501	112	214.2388	217.5087
30	505	112	210.3930	212.3652

The data presented in Table 1 show that all Nyberg construction S-boxes of length $N = 256$ based on the full set of irreducible polynomials have a nonlinearity distance of component Boolean functions $2N_S = 112$. However, different polynomials provide different values of nonlinearity in the sense of 4-functions and 16-functions. So, an S-box based on a polynomial $f_{19} = 419_{10}$ has the highest nonlinearity values of component 4-functions, while the S-box based on a polynomial $f_{16} = 395_{10}$ has the highest nonlinearity values of component 16-functions. Moreover, both nonlinearity values of the component 4-functions and the nonlinearity values of the component 16-functions of S-box based on the polynomial $f_{28} = 499_{10}$ are optimal. Earlier in [3], it was found that the polynomial $f_{28} = 499_{10}$ (however, like polynomial $f_9 = 355_{10}$) also provides the most uniform minimization of the matrix of correlation coefficients. From our perspective, this S-box can be recommended for practical use in the AES cryptographic algorithm from the point of view of nonlinearity criteria for component functions of many-valued logic [14].

5 Conclusions

Let us to summarize the main results of the research:

1. The nonlinearity values of component 4-functions and 16-functions of S-boxes of Nyberg construction of length $N = 256$ based on the full set of irreducible polynomials has been researched. It has been determined that the S-boxes of the Nyberg construction, which have the same nonlinearity distance of component Boolean functions, are at the same time characterized by different nonlinearity values of 4-functions and 16-functions for various irreducible polynomials. It was found that the nonlinearity values of the component 4-fucntions and component 16-functions of the S-box based on the polynomial $f_{28} = 499_{10}$ are optimal, therefore this polynomial can be recommended for practical use.
2. The method for researching the nonlinearity value of 4-functions was adapted to the case of 16-functions. This technique can be applied to S-boxes of other practically valuable constructions.
3. A recursive rule is proposed for constructing hexadecimal Vilenkin-Chrestenson matrices of an arbitrary order.

References

1. Nyberg K.: Differentially uniform mappings for cryptography. I Advances in cryptology. Proc. of EUROCRYPT’93. Berlin, Heidelberg, Lecture Notes in Compuer Springer-Verlag, New York,. Vol.765, pp. 55-65 (1994).
2. Schneier B.: Applied Cryptography. 2-nd edition. John Wiley & Sons, New York, p. 784 (1996).
3. Mazurkov M.I., Sokolov A.V.: Cryptographic properties of nonlinear transform of Rijndael cipher based on complete classes of irreducible polynomials. Odes’ kyi Politechnichnyi Universytet. Pratsi, No.2 (39), pp. 183-189 (2012).
4. Zhdanov O.N.: Key Information Selection Technique for Block Encryption Algorithm. INFRA-M, Moscow, p. 90 (2013).
5. Sokolov A., Zhdanov O.: Prospects for the Application of Many-Valued Logic Functions in Cryptography. International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, pp. 331-339 (2018).
6. Maier W., O.Staffelbach: Nonlinearity criteria for cryptographic functions. In Advances in Cryptology. EUROCRYPT’89, Lecture Notes in Computer Science, Springer-Verlag, vol.434, pp.549-562 (1990).
7. Logachev O.A., Salnikov A.A., Yashchenko V.V.: Boolean functions in coding theory and cryptology, Publishing house MTsNMO, Moscow, p. 472 (2004).
8. Sokolov A.V., Krasota N.I.: Very nonlinear permutations: synthesis methods for S-boxes with maximal 4-nonlinearity. Proceeding of ONAT named after A.S. Popov, Odessa, No. 1, pp. 145-154 (2017).
9. Trachtman A.M., Trachtman V.A.: Fundamentals of the theory of discrete signals on finite intervals. Soviet radio, Moscow, p. 208 (1975).
10. Tokareva, N.N.: Bent-functions: results and applications. Review of works. PDM, No. 1 (3), pp. 15-37 (2009).
11. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing, vol. 1126, pp. 93-104, 2020.
12. I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk and V. Tymchenko, Strumok key stream generator, IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 294-299.
13. Yeoh, W. -., Teh, J. S., & Sazali, M. I. “μ2: A lightweight block cipher”, Lecture Notes in Electrical Engineering, vol. 603, pp. 281-290, 2020, doi:10.1007/978-981-15-0058-9_27.
14. Zodpe H., Sapkal A. “FPGA-Based High-Performance Computing Platform for Cryptanalysis of AES Algorithm”, Advances in Intelligent Systems and Computing, Springer, vol. 1025, pp. 637-646, 2020.