Formation of shift index vectors of ring codes for information transmission security

Serhii Toliupa [1], Liubov Berkman [2], Serhiy Otrokh [1], Bohdan Zhurakovskyi [3], Valeriy Kuzminykh [3], and Hanna Dudarieva [2]

[1]Taras Shevchenko National University of Kyiv, Ukraine
[2]State University of Telecommunications, Kyiv, Ukraine
[3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

Abstract

The article discusses a method for converting ring codes into shift index vectors, which are designed to compress information and protect it from unauthorized access. The structure of the shift index vectors and the patterns of change in the decimal values of the shift index vectors are analyzed. The properties of shift index vectors created by transforming ring codes using binary transformations of the XOR, AND, OR elements of the initial sequence (first line) of the ring code and sequentially on each subsequent line are investigated. It has been established that the limits of change in the decimal values of the elements of the shift index vectors depend both on the length and number of ones in the code combinations of ring codes, and on the ratio of ones and zeros in the code combination. Analysis of the structure of shift index vectors of ring codes shows that for a family of ring codes of a certain type there is an unambiguous dependence of the decimal values of elements of shift index vectors and the limits of their location in the vector index on the number of elements and ones in the code combination. The set of decimal values of the shift index vector consists of three sequences. Using the family of ring codes like 000111 as an example, it is shown that the limits of each of the three sets are uniquely described depending on the ratio of the number of elements and ones in the codeword.

Keywords

Ring Codes, Shift Indexes Vector, Decimal Values

1. Introduction

The ring code is built on the principle of forming a cyclic code by shifting a certain number of elements to the right or left in the code combination and differs from the cyclic code that highest element of the code combination is shifted in place of the youngest element as if forming a ring. The ring code matrix is a square of size

$N \times N$, each line containing m ones and $N - m$ zeros [1-5]. At the same time each line of the matrix re-peats the previous line with a simultaneous ring shift of characters by a certain number of digits to the right or left. Based on the above, the ring code, which is formed by shifting one character of the code sequence from right to left, can be
represented as the following matrix G:

XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS-2021), December 9, 2021, Kyiv, Ukraine
EMAIL: tolupa@i.ua (S. Toliupa); berkmanlubov@gmail.com (L. Berkman); 2411197@ukr.net (S. Otrokh); zhurakovskiybyu@tk.kpi.ua (B. Zhurakovskyi); vakuz0202@gmail.com (V. Kuzminykh); Annett.13.86@gmail.com (H. Dudarieva)
ORCID: 0000-0002-1919-9174 (S. Toliupa); 0000-0002-6772-1596 (L. Berkman); 0000-0001-9008-0902 (S. Otrokh); 0000-0003-3990-5205(B. Zhurakovskyi); 0000-0002-8258-0816 (V. Kuzminykh); 0000-0002-9887-021X (H. Dudarieva)

$$G = \begin{bmatrix} k_{N-1}2^{N-1} + k_{N-2}2^{N-2} \ldots + k_1 2^1 + k_0 2^0 \\ k_{N-2}2^{N-1} + k_{N-3}2^{N-2} \ldots + k_0 2^1 + k_{N-1} 2^0 \\ . \\ . \\ . \\ k_0 2^{N-1} + k_{N-1}2^{N-2} \ldots + k_2 2^1 + k_1 2^0 \end{bmatrix}$$

where k is a binary element of the code combination, which takes on the value 0 or 1 depending on its structure.

According to [1-5] the ring code is characterized by a shift indexes vector (SIV), which is formed as follows:

- the binary logical transformation XOR, AND or OR is performed alternately over the elements of the first row and subsequent rows of the ring code matrix placed at the same positions of the code sequences. In this case the matrix of the ring code is converted into a shift indexes matrix;
- in each row of the resulting shift indexes matrix the number of elements corresponding to one is counted. At that, the shift indexes matrix transformed into a shift indexes vector.

The formula of transformation of matrix *G* into the shift indexes vector using the binary logical transformation XOR takes on the following form:

$$SIV_{XOR} = \begin{bmatrix} k_{N-1}2^{N-1} XOR\ k_{N-2}2^{N-1} + k_{N-2}2^{N-2} XOR\ k_{N-3}2^{N-2} + \cdots + k_0 2^0 XOR\ k_{N-1}2^0 \\ k_{N-1}2^{N-1} XOR\ k_{N-3}2^{N-1} + k_{N-2}2^{N-2} XOR\ k_{N-4}2^{N-2} + \cdots + k_0 2^0 XOR\ k_{N-2}2^0 \\ . \\ . \\ . \\ k_{N-1}2^{N-1} XOR\ k_0 2^{N-1} + k_{N-2}2^{N-2} XOR\ k_{N-1}2^{N-2} + \cdots + k_0 2^0 XOR\ k_1 2^0 \end{bmatrix}$$

The formula of transformation of matrix G into the shift indexes vector using the binary logical transformation AND takes on the following form:

$$SIV_{AND} = \begin{bmatrix} k_{N-1}2^{N-1} AND\ k_{N-2}2^{N-1} + k_{N-2}2^{N-2} AND\ k_{N-3}2^{N-2} + \cdots + k_0 2^0 AND\ k_{N-1}2^0 \\ k_{N-1}2^{N-1} AND\ k_{N-3}2^{N-1} + k_{N-2}2^{N-2} AND\ k_{N-4}2^{N-2} + \cdots + k_0 2^0 AND\ k_{N-2}2^0 \\ . \\ . \\ . \\ k_{N-1}2^{N-1} AND\ k_0 2^{N-1} + k_{N-2} AND\ k_{N-1}2^{N-2} + \cdots + k_0 2^0 AND\ k_1 2^0 \end{bmatrix}$$

The formula of transformation of matrix G into the shift indexes vector using the binary logical transformation OR takes on the following form:

$$SIV_{OR} = \begin{bmatrix} k_{N-1}2^{N-1} OR\ k_{N-2}2^{N-1} + k_{N-2}2^{N-2} OR\ k_{N-3}2^{N-2} + \cdots + k_0 2^0 OR\ k_{N-1}2^0 \\ k_{N-1}2^{N-1} OR\ k_{N-3}2^{N-1} + k_{N-2}2^{N-2} OR\ k_{N-4}2^{N-2} + \cdots + k_0 2^0 OR\ k_{N-2}2^0 \\ . \\ . \\ . \\ k_{N-1}2^{N-1} OR\ k_0 2^{N-1} + k_{N-2}2^{N-2} OR\ k_{N-1}2^{N-2} + \cdots + k_0 2^0 OR\ k_1 2^0 \end{bmatrix}$$

2. Analysis of the dependence of the shift index vectors structure on the type of the ring codes family

Each line (code sequence) of the ring code is characterized by a delta factor - the distribution of zeroes and ones between two extreme ones, separated by the largest number of zero symbols for a given initial vector. Ring codes having a delta factor of a particular type form a family of ring codes.

Each family of ring codes is characterized by the length of N code sequences and the number of *m* ones [6-8].

Each line (code sequence) of the ring code is characterized by a delta factor - the distribution of zeroes and ones between two extreme ones, separated by the largest number of zero symbols for a given initial vector. Ring codes having a delta factor of a particular type form a family of ring codes. Each family of ring codes is characterized by the length of N code sequences and the number of m ones [6-8].

In [9-11], the properties of families of ring codes are analyzed based on the delta factor of type 0011100 (ones in the code sequence are placed without interruption), type 010101 (ones and zeroes alternate) and type 001011. For these types of families of ring codes, mathematical models are built the formation of families based on the analysis of the values of code combinations in the decimal number system.

Table 1 shows the results of converting the families of ring codes of types 0011100, 010101, and 001011 to shift index vectors using the logical transformations XOR, AND and OR.

Table1.
Results of indexes ring codes to shear indexes vectors using logical transformations XOR, AND and OR

N	m	Structure of the ring code	XOR transformation		AND transformation		OR transformation	
			SIV structure	Sum	SIV structure	Sum	SIV structure	Sum
6	3	000111	24642	18	21012	6	45654	24
		001011	44244	18	11211	6	55455	24
		010101	60606	18	03030	6	63636	24
8	4	00001111	2468642	32	3210123	12	5678765	44
		00010111	4464644	32	2212122	12	6676766	44
		01010101	8080808	32	0404040	12	8484848	44
10	5	0000011111	2468108642	50	432101234	20	6789109876	70
		0000101111	446868644	50	332121233	20	778989877	70
		0101010101	10010010010010	50	050505050	20	10 5 10 5 10 5 10 5 10	70

Analysis of the structure of the shift index vectors allows us to conclude that, within the family of ring codes, the sequence of changes in the decimal values of the shift indexes vector is identical. The shift index vectors within the family differ in the number of decimal values and their values, which depend on the length of the codeword and the number of ones in each codeword.

Let us consider in greater detail the patterns of change in the values of the elements of the shift index vectors for family of the type 0011100.

3. Common factors of change in the values of shift indexes vector elements for ring codes family of the type 001110

Table 2 shows the results of transforming ring codes of the 0011100 family into shift index vectors using the logical transformations XOR, AND and OR. Fig. 1 shows a graph of the dependence of the decimal values of the elements of the shift index vectors, formed using the logical transformations XOR, AND and OR from the position number of their placement in the shift indexes vector V from right left. The graph is presented for the ring code of the 000111 family of length N = 7 with the number of ones m = 4.

Table 2.
Results of transforming ring codes of the 0011100 family into vectors of shift exponents using logical transformations XOR, AND and OR

N	m	Structure of the ring code	XOR transformation		AND transformation		OR transformation	
			SIV structure	Sum	SIV structure	Sum	SIV structure	Sum
	1	0000001	222222	12	000000	0	222222	12
	2	0000011	244442	20	100001	2	344443	22
7	3	0000111	246642	24	210012	6	456654	30
	4	0001111	246642	24	321123	12	567765	36
	5	0011111	244442	20	433334	20	677776	40
	6	0111111	222222	12	555555	30	777777	42
	1	00000001	2222222	14	0000000	0	2222222	14
	2	00000011	2444442	24	1000001	2	3444443	26
	3	00000111	2466642	30	2100012	6	4566654	36
8	4	00001111	2468642	32	3210123	12	5678765	44
	5	00011111	2466642	30	4322234	20	6788876	50
	6	00111111	2444442	24	5444445	30	7888887	54
	7	01111111	2222222	14	6666666	42	8888888	56
	1	000000001	22222222	16	00000000	0	22222222	16
	2	000000011	24444442	28	10000001	2	34444443	30
	3	000000111	24666642	36	21000012	6	45666654	36
9	4	000001111	24688642	40	32100123	12	56788765	36
	5	000011111	24688642	40	43211234	20	67899876	60
	6	000111111	24666642	36	54333345	30	78999987	66
	7	001111111	24444442	28	65555556	42	89999998	70
	8	011111111	22222222	16	77777777	56	99999999	72

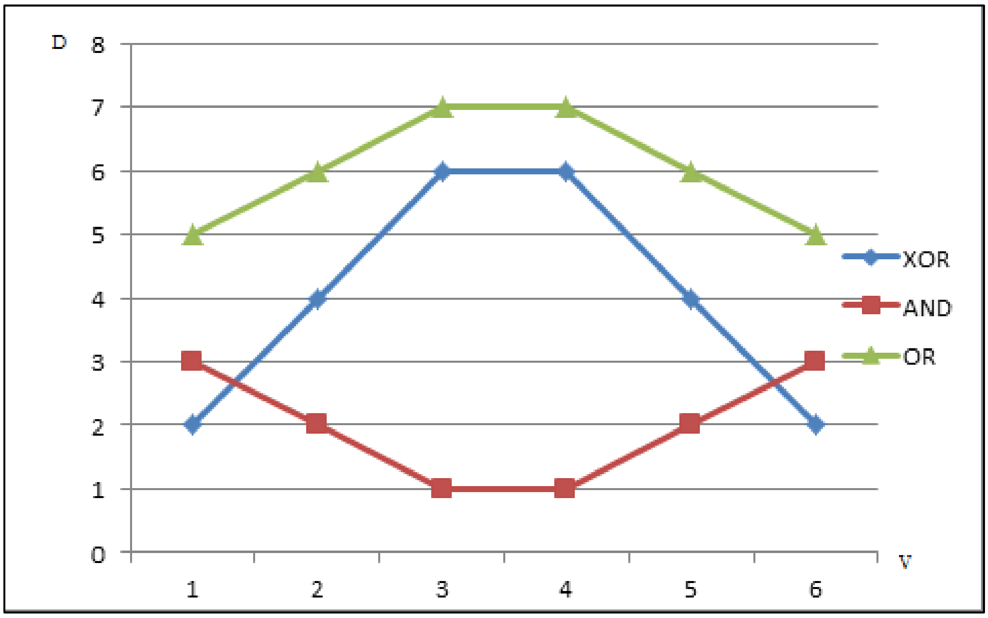

Figure 1. Graph of the dependence of the decimal values D of the elements of the shift index vectors from the position number of their placement in the shift indexes vector V

An analysis of the dependence of the decimal values D of the elements of the shift index vectors from the position number of their placement in the shift indexes vector V suggesting that the set of decimal values of the shift indexes vector PV consists of 3 subsets:

$$P_V = P_1 \cup P_2 \cup P_3,$$

where P_1 is a sequence of decimal values that are within the position of their placement in the shift indexes vector from left to right from 1 to *m* at $m \leq N\text{-}m$ and from 1 to *N*-*m* at $m > N\text{-}m$. In this case, *N* is the number of elements in the code combination, and *m* is the number of ones;

P_2 is a sequence of decimal values, located within the position of their placement in the shift indexes vector from left to right from m+1 to *N*-*m*-1 when *m*<*N*-m and from *N*-*m* +1 to m-1 when |*N*-2*m*| > 1. For |*N*-2*m*| ≤1, the sequence is zero;

P_3 is a sequence of decimal values that are within the position of their placement in the shift indexes vector from left to right from *N*-*m* to *N*-1 at *m*<*N*-*m* and from *m* to *N* -1 at *m*>*N*-*m*. Provided that *m* = *N*-*m*, the sequence P_3 is in the range of positions from *N*-*m* + 1 to *N*-1.In general, the mathematical model for determining the limits of the sequences P_1, P_2 and P_3 is as follows:

$$\lim_{n\to\infty} P_{1n} \in \begin{cases} [1, m], m \leq N - m; \\ [1, N - m], m > N - m. \end{cases}$$

$$\lim_{n\to\infty} P_{2n} \in \begin{cases} [m + 1, N - m - 1], m < N - m; \\ [N - m + 1, m - 1], \quad |N - 2m| > 1; \\ [\emptyset], |N - 2m| \leq 1. \end{cases}$$

$$\lim_{n\to\infty} P_{3n} \in \begin{cases} [N - m, N - 1], m < N - m; \\ [m, N - 1], m > N - m; \\ [N - m + 1, N - 1], \quad m = N - m. \end{cases}$$

Figure 2 shows the dependence of the values of the decimal values of the elements of the vectors of shift indicators on the number of the placement position in the shift indexes vector V, formed using the XOR logical operation of ring codes of the 011100 family with different codeword length *N* and the number of codeword ones *m* = 4.

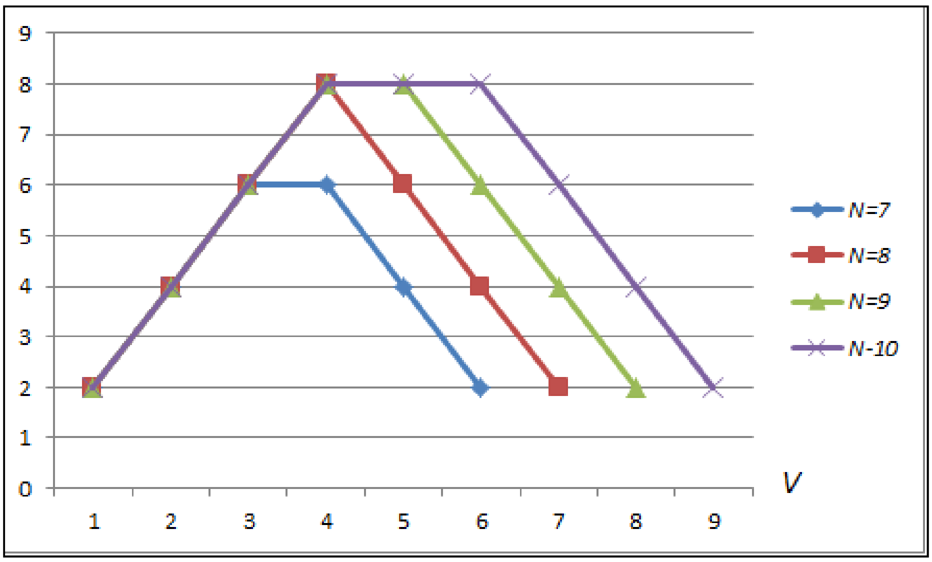

Figure 2. Graph of the dependence of the decimal values of the elements of the vectors of shift indicators on the position number of the placement in the shift index vectors, formed using the logical operation XOR for different lengths of code combinations *N*

Based on the analysis of the structure of the shift index vectors, it is possible to construct formulas for calculating the sums of the decimal values of the elements of the shift index vectors depending on the number of elements, the number of ones and zeros i*n* the code combination.

Below is a mathematical model for calculating the sums of decimal values of the elements of the vectors of displacement indicators, formed using the logical XOR transformation:

$$S_{XOR} = S_1 + S_2 + S_3 \ ,$$

where S_1 is the sum of the decimal values of the elements of the shift indexes vector, which is within the P_1 sequence; S_2 is the sum of the decimal values of the elements of the shift indexes vector, which is within the P_2 sequence; S_3 is the sum of the decimal values of the elements of the shift indexes vector, which is within the P_3 sequence.

Mathematical models for calculating the sums S_1, S_2 and S_3 are as follows:

$$S_1 = \begin{cases} \sum_{i=1}^{m} 2i, \ m \le N - m; \\ \sum_{i=1}^{N-m} 2i, \ m > N - m. \end{cases}$$

$$S_2 = \begin{cases} S_{2_1} + S_{2_2} + \dots + S_{2_{N-2m-1}}, \ S_{2_i} = 2m, m < N - m; \\ S_{2_1} + S_{2_2} + \dots + S_{2_{N-2m-1}}, S_{2_i} = 2(N - m), |N - 2m| > 1; \\ 0, |N - 2m| \le 1. \end{cases}$$

$$S_3 = \begin{cases} \sum_{i=0}^{m-1} 2m - 2i, \ m \le N - m; \\ \sum_{i=0}^{N-m-1} 2(N - m) - 2i, \ m > N - m. \end{cases}$$

where N is the number of elements in the code combination of the ring code, m is the number of ones in the code combination of the ring code.

4. Common factors of change in the values of shift indexes vector elements for ring codes family of the type 01010101

Table 3 shows the results of transforming ring codes of the 01010101 family into shift index vectors using the logical transformations XOR, AND and OR.

Fig. 2 shows a graph of the dependence of the decimal values of the elements of the vectors of shift indicators on the position number of the placement in the vector of 01010101 type shift index vectors, formed using the logical operation XOR for different lengths of code combinations *N*.

Table 3.
Results of transforming ring codes of the 01010101 family into shift index vectors using logical transformations XOR, AND and OR

N	m	Structure of the ring code	XOR transformation		AND transformation		OR transformation	
			SIV structure	Sum	SIV structure	Sum	SIV structure	Sum
8	3	00010101	6262626	30	0202020	6	6464646	36
	4	01010101	8080808	32	0404040	12	8484848	44
9	3	000010101	62644626	36	02011020	6	64655646	42
	4	001010101	82644628	40	03122130	12	85766758	52
10	3	0000010101	626464626	42	020101020	6	646565646	48
	4	0001010101	828282828	48	030303030	12	858585858	60
	5	0101010101	10010010010010	50	050505050	20	10510510510510	70

11	3	00000010101	6264664626	48	0201001020	6	6465665646	54
	4	00001010101	8284664828	56	0302112030	12	8586776858	68
	5	00101010101	102846648210	50	0413223140	20	106978879610	70
12	3	000000010101	62646664626	54	02010001020	6	64656665646	60
	4	000001010101	82848484828	64	03020202030	12	85868686858	76
	5	000101010101	10210210210210210	70	04040404040	20	10610610610610610	90
	6	010101010101	12012012012012012	72	06060606060	30	12612612612612612	102

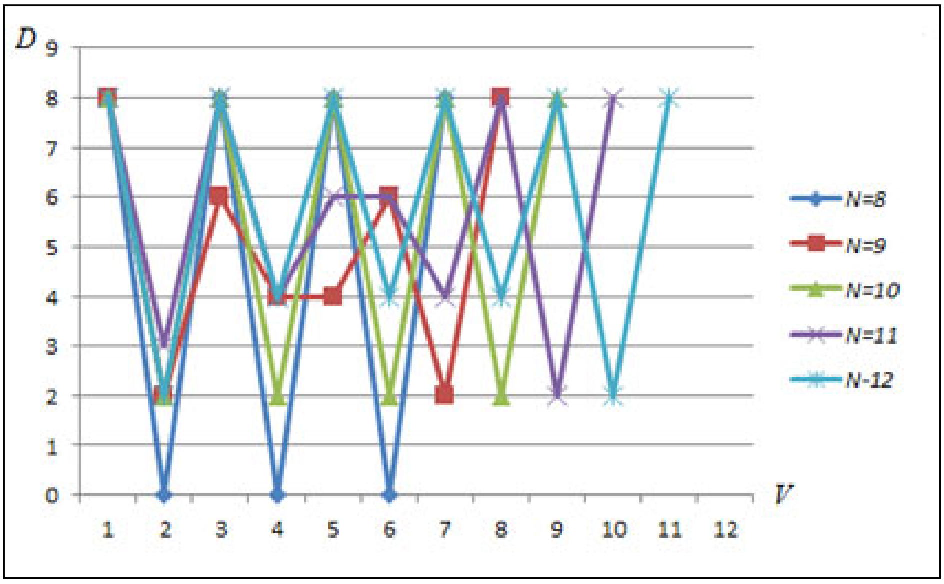

Figure 3. Graph of the dependence of the decimal values of the elements of the vectors of shift indicators on the position number of the placement in the vector of 01010101 type shift index vectors, formed using the logical operation XOR for different lengths of code combinations *N*

5. Common factors of change in the values of shift indexes vector elements for ring codes family of the type 1011100

Fig.4 shows a graph of the dependence of the decimal values of the elements of the vectors of displacement indicators, formed using the logical transformations XOR, AND and OR, from the position number of the placement in the vector of displacement indicators V from left to right. The graph is presented for the ring code of the family 000101111 of length N=9 with the number of symbols m=5.

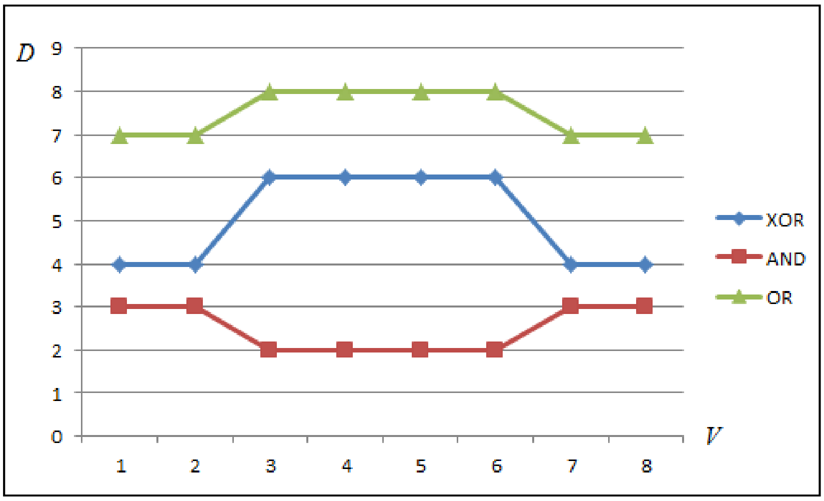

Figure 4. Graph of the dependence of the decimal values D of the elements of the shift index vectors from the position number of their placement in the shift indexes vector V

Table 4 shows the results of transforming ring codes of the 010111 family into shift index vectors using the logical transformations XOR, AND and OR.

Table 4.
Results of converting ring codes of the 0101111 family into shift index vectors using the logical transformations XOR, AND, and OR

N	m	Structure of the ring code	XOR transformation		AND transformation		OR transformation	
			SIV structure	Sum	SIV structure	Sum	SIV structure	Sum
	3	0001011	444444	24	111111	6	555555	30
7	4	0010111	444444	24	222222	12	666666	36
	5	0101111	424424	20	343343	20	767767	40
	3	00001011	4446444	30	1110111	6	5556555	36
	4	00010111	4464644	32	2212122	12	6676766	44
8	5	00101111	4446444	30	3332333	20	7778777	50
	6	01011111	4244424	24	4544454	30	8788878	54
	3	000001011	44466444	36	11100111	6	55566555	42
	4	000010111	44666644	40	22111122	12	66777766	52
9	5	000101111	44666644	40	33222233	20	77888877	60
	6	001011111	44466444	36	44433444	30	88899888	66
	7	010111111	42444424	28	56555565	42	98999989	70
	3	0000001011	444666444	42	111000111	6	555666555	48
	4	0000010111	446686644	48	221101122	12	667787766	60
	5	00000101111	446868644	50	332121233	20	778989877	70
10	6	0001011111	446686644	48	443323344	30	8899109988	78
	7	0010111111	444666444	42	555444555	42	999101010999	82
	8	0101111111	424444424	32	676666676	56	109101010101010910	88

Fig. 5 shows a graph of the dependence of the decimal values of the elements of the vectors of shift indicators on the position number of the placement in the vector of 00010111 type shift indexes.

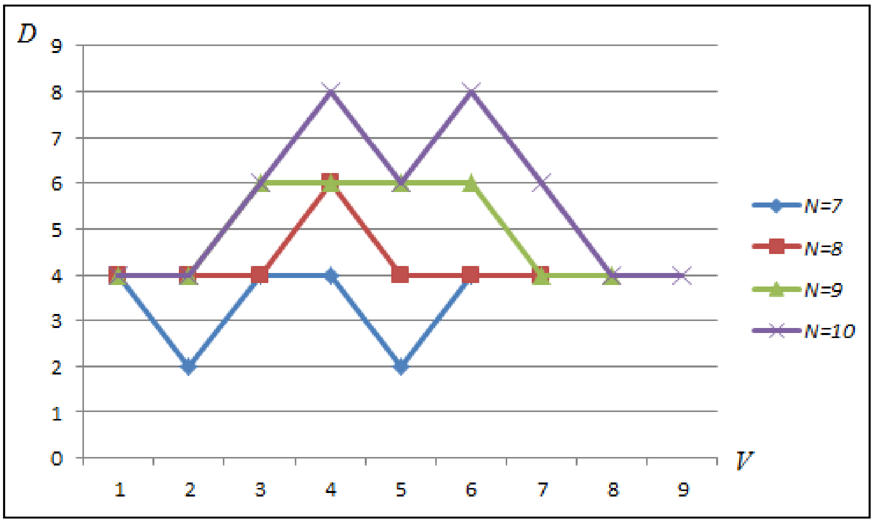

Figure 5. Graph of the dependence of the decimal values of the elements of the vectors of shift indicators on the position number of the placement in the vector of 0010111 type shift index vectors, formed using the logical operation XOR for different lengths of code combinations *N*

6. Conclusions

The method of converting ring codes into shift index vectors can be used to compress information transmitted over communication channels and improve the security of information transmission. In this case, at the receiving end of the communication channel, it is necessary to solve the problem of decoding the vector of shift indices into a ring code in order to obtain reliable information. The analysis of the structure of the shift index vectors, presented in this paper, allows you to see the patterns of change in the decimal values of the elements of the shift index vectors and their dependence on the length and the number of units in the code combination. An analysis of the change in the decimal values of the elements of the shift index vectors m, formed using logical XOR-transformations of the ring code of the type 011100, allows us to note that there is an unambiguous dependence of their decimal values on the number of elements N in the code combination, the number of ones m in the code combination and the value of the ratio of ones and zeros in each codeword of the ring code. At the same time, the limits of positions for placing the decimal values of the elements of the shift index vectors are uniquely defined. These patterns in the future makes it possible to develop the algorithm for converting shift index vectors into ring codes.

References

[1] V.B. Tolubko, S.I. Otrokh, L.N. Berkman, V.I. Kravchenko Manipulation coding of signal n-dimensional multi-position constellations based on the optimal noise immunity of regular structures– Kyiv: Telecomunication and information texnology –2017 – No 3(56) – p.5-11 (in Russian).

[2] S.I. Otrokh, V.A. Kuzminykh, I.O. Sosnovsky Future network in action, online life– Kyiv: Communication –2018 – No 6 – p.42-45 (in Russian).

[3] L.M. Hryshchenko Patterns of formation of ring codes. Mathematical model – Kyiv: Communication – 2016 – No 5(123). – p.27-31 (in Ukrainian).

[4] L.M. Hryshchenko Mathematical model for creating the 010101 type family ring code– Kyiv: Communication – 2017– No 1(125). – p.58-61 (in Ukrainian).

[5] E.V. Havrylko, S.I. Otrokh, V.I. Yarosh, L.M. Hryshchenko Improving the quality 8. of the future network by using the ring– Minsk: Communication Herald –2018 –No2 –p.60-64(in Russian).

[6] Security of information systems (in Russian) [Electronic Resource]. Mode of access: http://intuit.valrkl.ru/course-1312/index.html.

[7] S. Otrokh, V. Kuzminykh, O. Hryshchenko, Method of forming the ring codes// CEUR WorkshopProceedings - Vol-2318, - 2018, pp. 188-198.

[8] B. Zhurakovskyi, S. Toliupa, S. Otrokh, H.Dudarieva, V. Zhurakovskyi,
Coding for information systems security and viability //CEUR orkshop Proceedings, 2021,Vol - 2859, pp. 71–84.

[9] V. Tilavat, Y. Shukla, Simplification of procedure for decoding Reed–Solomon codes using various algorithms: an introductory survey. International Journal of Engineering Development and Research, 2(1), (2014). 279-283.

[10] D. Sarwate, R. Morrison, Decoder malfunction in BCH decoders. Information Theory, IEEE Transactions on, 36(4), 884-889.

[11] E. Richard, Blahut, "Algebraic Codes for Data Transmission", chapter 7.6 "Decoding in Time Domain", 2003.

[12] S. Lin, W. Chung, Y. Han, (2014, October). Novel polynomial basis and its application to reed-solomon erasure codes. In Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on (pp. 316-325). IEEE.

[13] Y. Wu. "Implementation of parallel and serial concatenated convolutional codes." Dissertation submitted to the Faculty of theVirginia Polytechnic Institute and State University. April, 2000. - 206 p.

[14] M.Vivek, N. Tilavat, Shukla Simplification of Procedure for Decoding Reed- Solomon Codes Using Various Algorithms: An Introductory Survey, 2014, INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH (IJEDR) (ISSN:2321-9939).

[15] M. Al-Bassam, A. Sonnino, V. Buterin, I. Khoffi, Fraud and Data Availability Proofs: Detecting Invalid Blocks in Light Clients. Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II, Mar 2021, Pages 279–298. https://doi.org/10.1007/978-3-662-64331-0_15.

[16] S.-J. Lin, W. Chung, Y. Han, Novel Polynomial Basis and Its Application to Reed-Solomon Erasure Codes. Published 13 April 2014, Computer Science, 2014 IEEE 55th Annual Symposium on Foundations of Computer Science. Conference Paper | Publisher: IEEE. Cited by: Papers (26).