Jurnal Pendidikan Matematika Vol: 2, No 1, 2024, Page: 1-9

Analysis of the Application of Logical Operations to Cryptographic Transformations of Information Security Means

M. M. Madaminov[1*], A. F. Farhodjonov

[12] Kokand State Pedagogical Institute

DOI:
https://doi.org/10.47134/ppm.v21.1024
*Correspondence: M. M. Madaminov
Email:
muslimbekmadaminov19@gmail.com

Received: 20-09-2024
Accepted: 20-10-2024
Published: 21-11-2024

Abstract: In the article, the solution to the problem of determining logical operations that ensure cryptographic stability of the transformation of algorithms of cryptographic methods of information security is justified by the criterion of regularity - equal distribution"0" and "1" in the truth table. A logical operation with a truth table of uniform distribution of "0" and "1" and or blocks of bits has the property of cryptographic resistance.

Keywords: Cryptology, Cryptographic Algorithm, Cryptographic Strength, Symmetric Encryption, Opening Key, Disjunction, Conjunction, Transformations, Microprocessor, Boolean Function.

Introduction

The fundamentals of digital technology and information exchange technology in information and communication networks are closely linked by electronic means based on logical operations. The so-called microprocessor, microcontroller, chip, integrated circuits and other electronic developments are the foundations of modern computing, control, hardware and hardware-software control means.

Statement of the problem

This article examines the issues of cryptographic strength, efficient hardware and hardware-software feasibility of cryptographic transformations based on logical operations performed on bits and blocks of bits of the blocks being transformed (Pang, 2022).

Methodology

Solution to the problem.

It is noted that the operation is necessarily used in the main transformations of ideally stable and stable encryption algorithms $\oplus$ −XOR[6-10]. Operati $x \oplus y = z$ on is determined: if $x = 0$ and $y = 0$ or $x = 1$ and $y = 1$, that $z = 1$; otherwise $z = 0$. The truth table has the following form:

x◎y	0	1
0	0	1
1	1	0

From the truth table it is clear that z- representing the result of four possible variants of this operation takes the values “0” and “1” with equal distribution, i.e. in the values z “0” and “1” are repeated twice. In general, the number of operations between two variables x and y equals $2^4 = 16$. Indeed, there are 4 different combinations of the pair's meaning x and y: $x = 0$ and $y = 0$; $x = 1$ and $y = 0$; $x = 0$ and $y = 1$; $x = 1$ and $y = 1$. The values of the pair yield 4 values z_1,z_2,z_3 and z_4, which takes the values “0” or “1”. This means that four bits $(z_1 z_2 z_3 z_4)$ can be coded $2^4 = 16$ different values: $(0000)_2 = (0)_{10}$, $(0001)_2 = (1)_{10}$, …, $(1110)_2 = (14)_{10}$,
$(1111)_2 = (15)_{10}$.
For surgery $\oplus$ −XOR according to its truth table state:

x * 9 y	0	1
0	0	1
1	1	0

we can put in correspondence the number $(0110)_2$ =6. Thus, we can introduce logical operations corresponding to the following states of the truth table: $(0000)_2$ =0, $(0001)_2$ =1, $(0010)_2$ =2, $(0011)_2$ =3, $(0100)_2$ =4, $(0101)_2$ =5, $(0110)_2$ =6, $(0111)_2$ =7, $(1000)_2$ =8, $(1001)_2$ =9, $(1010)_2$ =10, $(1011)_2$=11, $(1100)_2$ =12, $(1101)_2$ =13, $(1110)_2$ =14, $(1111)_2$ =15. Where the logical operations $*_0$ and $*_{15}$ correspond to the states $(0000)_2$ =0 and $(1111)_2$ =15 with the following truth tables

x◎₀◎y	0	1
0	0	0
1	0	0

and

x◎₁₅◎y	0	1
0	1	1
1	1	1

do not have the property of effective mixing [6-10]. Since whatever the encrypted block or key block, the results of the transformation by these logical operations will contain blocks of the sequence of only "0"-zeros or "1"-units. This circumstance allows for the fabrication of false ciphers. Therefore, the use of operations $*_0$ and $*_{15}$ in cryptographic transformations is inappropriate (Ryu, 2022).
Here, for clarity, are given the truth tables corresponding to the operations $*_1$- conjunction and $*_7$-disjunction.

$x \circledcirc_{\circledcirc} y$	0	1
0	0	0
1	0	1

and

$x \circledcirc_{\circledcirc} y$	0	1
0	0	1
1	1	1

Thus, over two variables, in addition to the operation $*_0$ and $*_{15}$, it is possible to define 14 (fourteen) operations. In addition, the operations are defined by the following truth tables:

x $*_3$ y	0	1
0	0	0
1	1	1

and

$x*_5$ y	0	1
0	0	1
1	0	1

are unstable, since the first $x *_3 y = z$ leaves unchanged x, and the second x $*_5$ y remains unchanged$y$. This circumstance occurs because in the first table the row corresponding to the value of the variable $x = 0$ has elements only with value 0-zero, and a string with value $x = 1$ has elements with value 1-one only, Similarly, in the second table the column corresponding to the value of the variable $y = 0$ has elements only with value 0-zero, and a column with value $y = 1$ has elements with value 1-one only (Mikhalycheva, 2024). Other operations can perform mixing transformations on the bits of the open or intermediate blocks with the corresponding bits of the key block (Moldovyan, 2004).

Below is a comparison table of the introduced logical operations with respect to the features of the cryptographic resistance property. In this table, the cryptographic resistance of the following operations is substantiated by comparison: $x *_9 y=z$, $x *_{10} y=z$, $x *_{12} y=z$. These operations, together with the operation x⊕y =x$*_6$ y=z, can be widely used as secure transformations.

No. P/P	Operation type	Truth table of the operation			Analysis of possible states of the operation result	Comment
1	$x*_1 y=z$	$x \setminus y$	0	1	1) The values of the result z are not uniformly distributed:	Relatively stable.
		0	0	0	2) The value z=0 corresponds to 3 (three) values of the pair of variables x and y, and z=1 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=1 it follows that	
		1	0	1		
2	$x*_2 y=z$	**$x \setminus y$**	**0**	**1**	**1) The values of the result z are not uniformly distributed:**	Relatively stable.
		0	**0**	**0**	**2) The value z=0 corresponds to 3 (three) values of the pair of variables x and y, and z=1 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=1 it follows that x=1 and y=0.**	
		1	**1**	**0**		
3	$x*_4 y=z$	**$x \setminus y$**	**0**	**1**	**1) The values of the result z are not uniformly distributed:**	Relatively stable
		0	**0**	**1**	**2) The value z=0 corresponds to 3 (three) values of the pair of variables x and y, and z=1 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=1 it follows that x=0 and y=1.**	
		1	**0**	**0**		
4	$x*_6 y=z$	**$x \setminus y$**	**0**	**1**	**1) The result values z are uniformly distributed;**	**Resistant**
	$x \circledcirc\circledcirc y \circledcirc z$	**0**	**0**	**1**	**2) The values z=0 and z=1 correspond to 2 (two) values of the pair of variables x and y, i.e. there are 4 (four) unknown states.**	
		1	**1**	**0**		

5	$x*_7$y=z	x \ y	0	1	1) The values of the result z are not uniformly distributed: 2) The value z=1 corresponds to 3 (three) values of the pair of variables x and y, and z=0 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=0 it follows that x=0 and y=0.	Relatively stable
		0	0	1		
		1	1	1		
6	$x*_8$y=z	**x\ y**	**0**	**1**	**1) The values of the result z are not uniformly distributed: 2) The value z=0 corresponds to 3 (three) values of the pair of variables x and y, and z=1 corresponds to the value of 1 (one) pair, there are 3 (three) unknown states, i.e. from z=1 it follows that x=0 and y=0.**	Relatively stable
		0	**1**	**0**		
		1	**0**	**0**		
7	$x *_9 y = z$	x \ y	0	1	1) The result values z are uniformly distributed; 2) The values z=0 and z=1 correspond to 2 (two) values of the pair of variables x and y, i.e. there are 4 (four) unknown states.	**Resistant**
		0	1	0		
		1	0	1		
8	$x*_{10}$y=z	**x\ y**	**0**	**1**	**1) The result values z are uniformly distributed; 2) The values z=0 and z=1 correspond to 2 (two) values of the pair of variables x and y, i.e. there are 4 (four) unknown states.**	**Resistant**
		0	**1**	**0**		
		1	**1**	**0**		
9	$x*_{11}$y=z	x \ y	0	1	1) The values of the result z are not uniformly distributed: 2) The value z=1 corresponds to 3 (three) values of the pair of variables x and y, and z=0 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=0 it follows that x=0 and y=1.	Relatively stable
		0	1	0		
		1	1	1		
10	$x*_{12}$y=z	**x\ y**	**0**	**1**	**1) The result values z are uniformly distributed; 2) The values z=0 and z=1 correspond to 2 (two) values of the pair of variables x and y, i.e. there are 4 (four) unknown states.**	**Resistant**
		0	**1**	**1**		
		1	**0**	**0**		
11	$x*_{13}y=z$	x \ y	0	1	1) The values of the result z are not uniformly distributed: 2) The value z=1 corresponds to 3 (three) values of the pair of variables x and y, and z=0 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=0 it follows that x=1 and y=0.	Relatively stable
		0	1	1		
		1	0	1		
12	$x*_{14}$y=z	**x\ y**	**0**	**1**	**1) The values of the result z are not uniformly distributed: 2) The value z=1 corresponds to 3 (three) values of the pair of variables x and y, and z=0 corresponds to the value 1 (one) pair, there are 3 (three) unknown states, i.e. from z=0 it follows that x=1 and y=1.**	Relatively stable
		0	**1**	**1**		
		1	**1**	**0**		

This comparison table substantiates the cryptographic strength of the following operations: $x*_9$ y=z, $x*_{10}$ y=z, $x*_{12}$ y=z. These operations, together with the operation $x \oplus y = x *_6 y = z$, can be widely used as strong transformations.

The relative stability of the disjunction operation is determined $x \cup y = x *_7 y = z$ and the conjunction $x \cap y = x *_1 y = z$.

Using certain persistent operations, it is possible to perform bitwise transformations on blocks $x = (x_1x_2x_3x_4...x_n)$ and $y = (y_1y_2y_3y_4...y_n)$, $n \geq 2$, i.e.

$$x *_i y = \begin{cases} x_1 x_2 \dots x_n \\ *_i \\ y_1 y_2 \dots y_n \\ \hline z_1 z_2 \dots z_n \end{cases}, i=6,9,10,12.$$

In this case, you can make sure that different pairs of blocks (x, y), Where $x = (x_1 x_2 x_3 x_4 ... x_n)$ and $y = (y_1 y_2 y_3 y_4 ... y_n)$, correspond to different $z = (z_1 z_2 z_3 z_4 ... z_n)$. This means that the results of the transformation carried out by stable certain operations have the property of regularity [6]. And the transformations carried out by relatively stable operations do not have (or do not fully have) the property of regularity. These statements are verified by direct calculation (Zhang, 2023). Below are examples of transformations with a stable and relatively stable operation, when the length of the transformed block for simplicity $n = 2$. Then over the corresponding bits of the variables $x = (x_1 x_2)$ and $y = (y_1 y_2)$ by performing logical operations, we get results $z = (z_1 z_2)$.

$x \backslash y$	0	1
0	0	0
1	1	1
x	y	x◎$_{◎}$y ◎◎
00	00	00
01	00	01
10	00	10
11	00	11
00	01	00
01	01	01
10	01	10
11	01	11
00	10	00
01	10	01
10	10	10
11	10	11
00	11	00
01	11	01
10	11	10

$x \backslash y$	0	1
0	1	0
1	0	1
x	y	x◎$_{◎}$y ◎◎
00	00	11
01	00	10
10	00	01
11	00	00
00	01	10
01	01	11
10	01	00
11	01	01
00	10	01
01	10	00
10	10	11
11	10	10
00	11	00
01	11	01
10	11	10

$x \backslash y$	0	1
0	0	0
1	0	1
x	y	x◎$_{◎}$y ◎◎
00	00	00
01	00	00
10	00	00
11	00	01
00	01	00
01	01	01
10	01	00
11	01	01
00	10	00
01	10	00
10	10	10
11	10	10
00	11	00
01	11	01
10	11	10

$x \backslash y$	0	1
0	0	1
1	1	1
X	y	x◎$_{◎}$y ◎◎
00	00	00
01	00	01
10	00	10
11	00	11
00	01	01
01	01	01
10	01	11
11	01	11
00	10	10
01	10	11
10	10	10
11	10	11
00	11	11
01	11	11
10	11	11

11	11	11

11	11	11

11	11	11

11	11	11

In these examples the first transformation is carried out by an unstable operation, the second is carried out with a stable operation and therefore it is clear that it has the property of regularity (Akhmedova, 2022). The next two transformations are carried out with relatively stable operations and do not have the property of regularity.

Similarly, one can introduce operations based on a truth table with blocks of two bits: "00", "01", "10", "11". The number of possible truth tables is 416 = 4 294 967 296. If these pairs of bits are distributed uniformly on a 4×4 truth table, in addition to the row corresponding to the value of the variable $x = x_1^i x_2^j$, where $i = 0,1$; and $j = 0,1$; there are elements not only with the meaning "$x_i^i x_2^j$", similarly in the column corresponding to the value of the variable$y = y_1^i y_2^j$there are elements not only with the meaning "$y_1^i y_2^j$", for example:

$x *_i y$	00	**01**	**10**	**11**
00	01	10	00	11
01	11	01	10	00
10	00	11	01	10
11	11	00	11	01

then the defined operations will have cryptographic efficiency—the property of resistance. The number of truth tables with uniform distribution of "00", "01", "10", "11"—pairs of bits

$$C_{16}^4 = \frac{16!}{4!\ 12!} = \frac{13 \cdot 14 \cdot 15 \cdot 16}{2 \cdot 3 \cdot 4} = 13 \cdot 7 \cdot 5 \cdot 4 = 1820$$

Of these, tables with rows and tables with the same elements are also excluded, their number is 8. Thus, it is possible to introduce 1820-8=1812 operations with the property of uniform distribution of the value: "00", "01", "10", "11" and cryptographic strong features. In the same way, based on blocks with three bits of different 23 = 8 elements "000", "001", "010", "011", "100", "101", "110", "111" truth table of size 8×8, it is possible to introduce 864 operations. Of these, the number of truth tables with uniform distribution with three bits of different 2^3 = 8 elements

$$C_{64}^8 = \frac{64!}{8!\ 56!} = \frac{57 \cdot 58 \cdot 59 \cdot 60 \cdot 61 \cdot 62 \cdot 63 \cdot 64}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} = 19 \cdot 29 \cdot 59 \cdot 15 \cdot 61 \cdot 31 \cdot 3 \cdot 8 = 22\,130\,826\,840$$

The number of truth tables cryptographic strong features

$$C_{64}^8 - 16 = 22\,130\,826\,840 - 16 = 22\,130\,826\,824$$

In the scientific works [9,11,12] of the authors of the proposed article, a compression table of the byte “2 13” = “0010 1011” on the half byte “10” = “1010”, i.e. at the intersection of row 2 with column 13 according to the following table is given:

y / x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	5	13	6	11	1	10	15	8	0	4	7	9	2	12	3	14
1	8	7	2	14	15	3	11	6	1	12	13	10	5	4	9	0
2	14	2	13	4	12	7	1	11	6	9	0	5	3	10	8	15
3	0	14	9	12	3	13	7	4	15	6	5	1	11	2	10	8
4	3	10	7	2	4	12	9	1	14	13	15	8	0	5	11	6
5	2	3	1	8	0	14	5	9	12	11	6	7	10	15	13	4
6	10	4	14	15	9	5	8	2	11	0	1	3	12	6	7	13
7	11	9	10	1	6	4	13	15	3	5	14	0	8	7	2	12
8	1	0	3	7	13	11	10	12	9	14	4	6	15	8	5	2
9	4	8	11	9	14	6	2	5	10	3	12	15	7	13	0	1
10	9	12	15	0	2	1	14	10	5	8	11	13	4	3	6	7
11	6	11	8	13	7	9	0	3	4	15	10	2	14	1	12	5
12	15	1	0	5	10	8	3	7	13	2	9	12	6	14	4	11
13	12	5	4	10	11	2	6	13	8	7	3	14	1	0	15	9
14	7	15	12	6	5	0	4	14	2	10	8	11	13	9	1	3
15	13	6	5	3	8	15	12	0	7	1	2	4	9	11	14	10

In this table, the numbers from 0 to 15, which are expressed with four bits, are distributed uniformly, i.e. they are repeated exactly 16 times, and are repeated once in each row and column. Of such tables, taking as truth tables the operations on blocks of four bits of different elements "0000", "0001", "0010", "0011", "0100", "0101", "0110", "0111", "1000", "1001", "1010", "1011", "1100", "1101", "1110", "1111" can be introduced 16256 operations. From such truth tables with uniform distribution with four bits of different $2^4 = 16$ elements can be distinguished in the amount of $C_{256}^{16} = \frac{256!}{16!\,240!}$, which gives a huge amount $C_{256}^{16} - 32 = \frac{256!}{16!\,240!} - 32$ logical operations with strong cryptographic properties.

Result and Discussion

Any transformation is carried out on the basis of some operation or their sequence. If the transformation puts different possible input values in correspondence with different possible values or with an equal distribution of all possible values, then it is said to have the property of regularity (Yu, 2023). A transformation that has the property of regularity has the property of resistance, i.e. when solving the problem of revealing the ciphers of encrypted blocks, it is necessary to select all possible options (Rasheed, 2024). The logical operation has this property $\oplus$ −XOR. The article defines and justifies the regularity of a number of logical operations on bits and blocks of bits that can be used with such cryptographic success as the operation $\oplus$ −XOR in the development of cryptographic algorithms and their software and hardware (Babenko, 2024). The implementation of these operations on bits and blocks of bits will ensure the exchange of digital signals without delays in hardware and hardware-software implementations of cryptographic algorithms.

Conclusion

In the proposed article, the variables x and y, variable z, expressing the result, take the values “0” or “1”, also blocks of bits. The number of possible operations on the expression is determined$x * y = z$in accordance with different possible truth tables. In the case of an operation on bits, logical operations ($*_i$, i=1,2,…,16) are conditionally mapped to different truth tables. It is substantiated that if in the truth tables of the introduced operations the values “0” and “1” are distributed uniformly repeated in equal quantities, then the bit-by-bit transformation of blocks, carried out on the basis of such operations, have the property of regularity (K, 2024). Such a substantiation is asserted for an operation on blocks of bits. The obtained results, in addition to solving problems of cryptographic protection of information, have a wide application in various fields of science, information technology and technology.

References

A.V. Frunze "Microcontrollers? It's so simple!" 1-3 Vol. Moscow: LLC "IV SKIMAN", 2002

Akbarov D.E. Akhborot havfsizligini taminlashning cryptographic usullari va ularning qўllanilishi – Toshkent, “Uzbekiston Markasi”, 2009 – 434 bet.

Akbarov D. E., Umarov Sh. A. Hash function algorithm with new basic transformations. // Bulletin of the National Technical University "Kyiv Polytechnic Institute". http//visnykpb.kpi.ua/ru/journal. National Technical University. -№ 1(51). 2016, -pp. 100-108

Akbarov D. E., Umarov Sh. A. Development of a new algorithm for data encryption with a symmetric key. // Journal of Siberian Federal University. Engineering & Technologies -2016, No. 9(2). - p. 214-224.

Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. Fundamentals of cryptography: Textbook, 2nd ed. – M.: Helios ARV, 2002.-480 p

Akhmedova, L. S. (2022). Application of logical and mathematical methods for the analysis of environmental information. *South of Russia: Ecology, Development*, *17*(4), 206–211. https://doi.org/10.18470/1992-1098-2022-4-206-211

Babenko, V. (2024). Information-Driven Permutation Operations for Cryptographic Transformation. *CEUR Workshop Proceedings*, *3654*, 137–149. https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85189137528&origin=inward

Brodin V.B., Kalinin A.V. "Systems on microcontrollers and LSI programmable logic" Moscow: "ECOM" 2002.

K, C. K. V. (2024). A novel deep learning technique with cryptographic transformation for enhancing data security in cloud environments. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-18903-8

Mikhalycheva, E. A. (2024). Application of Probabilistic Safety Analysis to the Emergency Scenarios Assessment of a Loss of Coolant Accidents in the VVER-Reactor Plant. *Nonlinear Phenomena in Complex Systems*, *27*(1), 69–77. https://doi.org/10.5281/zenodo.10889768

Moldovyan N.A., Moldovyan A.A., Eremeev M.A. Cryptography: from primitives for the synthesis of algorithms. – SPb.: BHV-Petersburg, 2004. - 448 p.

Pang, C. (2022). Research and Application of Tax Classification Prediction Analysis Method Based on Big Data Technology. *Lecture Notes on Data Engineering and Communications Technologies*, *102*, 413–421. https://doi.org/10.1007/978-981-16-7466-2_46

Rasheed, A. M. (2024). Lightweight Cryptographic Algorithms for Medical IoT Devices using Combined Transformation and Expansion (CTE) and Dynamic Chaotic System. *International Journal of Advanced Computer Science and Applications*, *15*(4), 705–715. https://doi.org/10.14569/IJACSA.2024.0150472

Ryu, C. H. (2022). Modern applications of scanning electrochemical microscopy in the analysis of electrocatalytic surface reactions. *Chinese Journal of Catalysis*, *43*(1), 59–70. https://doi.org/10.1016/S1872-2067(21)63948-7

Schneier B. Applied cryptography. Protocols, algorithms, source texts in C. –M.: TRIUMF Publishing House, 2003 - 816 p.

Shalyto A.A. Logical control. Methods of hardware and software implementation. – St. Petersburg: , 1999. -779 p.

V.N. Baranov. "Application of AVR microcontrollers: circuits, algorithms, programs". Moscow, 2004. - 288 p.

Yu, Z. (2023). Application of Combinatorics Based on Discrete Analysis in WCET Embedded Software Testing Technology. *Lecture Notes in Electrical Engineering*, *1063*, 27–35. https://doi.org/10.1007/978-981-99-4554-2_4

Zenzin O. S., Ivanov M. A. Cryptographic Security Standard – AES. Finite Fields / Edited by M. A. Ivanov – M.: KUDITS-OBRAZ, 2002. - 176 p.

Zhang, H. (2023). Application of Python Scientific computing library and Simulation in Circuit Analysis. *Proceedings - 2023 12th IEEE International Conference on Communication Systems and Network Technologies, CSNT 2023*, 892–898. https://doi.org/10.1109/CSNT57126.2023.10134600