ISSN NO: 2770-4491
Date of Publication:20-12-2022

Building Models of Their Functions According to Single-Valued and Multivalued Compatibility Truth Table of Cryptographic Accelerations

Khasanov Khayrullo Makhmudovich
Kokand State Pedagogical Institute, Uzbekistan.

Annotation: The article describes the features and properties of constructing models of these functions according to the truth table of single-valued and multi-valued cryptographic representations.

Keywords: Table, boolean function, chorus operation, examples

Information and communication networks, the construction of models of cryptographic reflections in the form of non-linear features, which provide cryptographically effective mixing and distribution of data blocks, greatly facilitates the creation of hardware devices [1, 2] . And BF they are modeled on the basis of the truth table [3, 4, 5]. Due to the increase in the number of reflection variables, the size of the truth table increases dramatically , complicating the process of building a BF model. However, given a reflection truth table, a general method of constructing its Boolean function was developed [4].

In this article, it is shown that regardless of the number of reflection variables $n = 4, 8, 16, 32, 64, 128,$, etc., and the size of the truth table increases dramatically, it is possible to build a boolean function model of the reflection without relying on its truth table expression, based on the properties of the reflection itself, while maintaining the cryptoresistance properties.

It is known that most cryptographic algorithms $n = 16, 32, 64, 128$ use reflections, which are the number of variables [4, 6, 7].

general, encryption algorithm $GF(2)^n = \{x = (x_1, x_2, ..., x_n) \in X : x_i \in \{0;1\}\}$ mappings $GF(2)^m = \{y = (y_1, y_2, ..., y_m) \in Y : y_i \in \{0;1\}\}$ can be expressed in the form of functions as follows:

$Y = f(X): GF(2)^n \to GF(2)^m$,

where the vector-function $f(x)$ is represented in the form of $x_i, y_i \in GF(2) = \{f_1(x), f_2(x), ..., f_m(x)\}$, that is, $x_i, y_i = \{0;1\}$.

The so-called algebraic normal form (ANF) for BF expressions is as follows

$$f(x) = a_0 \oplus \sum_{1 \le i \le n} a_i x_i \oplus \sum_{1 \le i_1 < i_2 \le n} a_{i_1 i_2} x_{i_1} x_{i_2} \oplus ... \oplus \sum_{1 \le i_1 < ... < i_2 \le k} a_{i_1 ... i_k} \oplus ... \oplus a_{12...n} x_1 x_2 ... x_n, \qquad (1)$$

where $x \in GF(2)^n$ and coefficients $a_0, a_i, a_{i_1 i_2}, ..., a_{12...n} \in GF(2)$, the view is used [3] .

In many cases, for example: in S-blocks of the DES encryption algorithm, in reflections based on the compression table [6, 7], in hash-function algorithms, in reflections carried out by performing algebraic operations, work is done $n > m$ on the basis of permutations and substitutions that can be expressed by the function satisfying the condition $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_m)$. It is necessary to construct functional models of such reflections $(x_1, x_2, \ldots, x_n)$- to all values $(f_1, f_2, \ldots, f_m)$of vectors - to define some values of vectors corresponding to repetition. That is, the -components in the $n > m$exact $n = m$state are f_j combined with arbitrary *m* (*j* =1, ... *m ;) or m* selected taking into account some properties of the truth table , each of which consists of the conjugation of all $x_i (i = 1, 2, \ldots, n)$ variables themselves or their negations $2^n : 2 = 2^{n-1}$. of dissimilar values $\oplus$ - defined by Boolean functions of the form (1) expressed by the XOR operation. Such identification of reflections *It can be verified* by direct definition that it provides the properties of *nonlinearity* and regularity given in [3] .

E -expansion of the DES encryption algorithm in the tabular permutation, such as the mapping of the 8 *-bit number in the S -block of the Blowfish crypto-algorithm* to a 32 *-bit* number, permutations and

ISSN NO: 2770-4491
Date of Publication:20-12-2022

replacements $n < m$ are represented by a function that satisfies the condition . $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_m)$ As above, in this $n = m$ case f_j, arbitrary *n of -components* (*j* =1, ... *n ;) or n* selected taking into account some properties of the truth table, each of them is combined with pairs consisting of the conjunction of all $x_i (i = 1, 2, \ldots, n)$ variables themselves or their negations $2^n : 2 = 2^{n-1}$ of dissimilar values $\oplus$ - defined by Boolean functions of the form (1) expressed by the XOR operation. of -hads formed $x_1^{(t)} \ldots x_k^{(t)} \ldots x_n^{(t)}$ from conjunctions, here $1 \le k \le n;\ x_k^{(t)} \in \{x_k, \bar{x}_k\} \left(1 \le t \le 2^{n-1}\right)$, the number of pairwise different ones is 2^n ta, the f_j number 2^{n-1} of terms of the expression of the -components functions is ta, the number 2^n of different combinations made from $C_{2^n}^{2^{n-1}}$ ta elements is calculated by this $2^{n-1} = \frac{(2^n)!}{(2^{n-1})!(2^n - 2^{n-1})!} = \frac{(2^n)!}{(2^{n-1})!(2^{n-1})!}$ formula. This calculated value is sufficiently larger than the numbers *n* and . 2^n For example *n* =4 and 2^n=16, $C_{16}^8 = \frac{(16)!}{(8)!(8)!}$ =4290. Therefore, it is not a problem to determine the -components of the $n < m$ function f_j satisfying the condition $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_m)$ according to the above requirements.

is a method that allows you to build a function model without relying on its truth table when there are a number of reflection variables , etc. *n* = 4, 8, 16, 32, 64, 128,

According to this one-valued correspondence truth test when A) . $n = m = 4$

	1
	3
	5
	4
0	
1	2
2	0
3	
4	
5	

its $f(x_1, x_2, x_3, x_4) = (f_1, f_2, f_3, f_4)$ boolean function model is as follows [4, 5]:

ISSN NO: 2770-4491
Date of Publication:20-12-2022

$f_1 = \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 x_3 \bar{x}_4 \oplus x_1 \bar{x}_2 x_3 x_4 \oplus x_1 x_2 \bar{x}_3 \bar{x}_4 \oplus x_1 x_2 x_3 x_4$;

$f_2 = \bar{x}_1 \bar{x}_2 x_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 \bar{x}_3 x_4 \oplus x_1 \bar{x}_2 x_3 x_4 \oplus x_1 x_2 x_3 \bar{x}_4$;

$f_3 = \bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 \bar{x}_3 x_4 \oplus x_1 x_2 \bar{x}_3 \bar{x}_4$;

$f_4 = \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus x_1 x_2 \bar{x}_3 x_4 \oplus x_1 x_2 x_3 \bar{x}_4 \oplus x_1 x_2 x_3 x_4$.

B) $n = 4 > m = 2$ according to this multi-valued matching truth test

0	
1	
2	
3	
4	
5	

its $f(x_1, x_2, x_3, x_4) = (f_1, f_2)$ boolean function model would be:

$f_1 = \bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 x_2 \bar{x}_3 \bar{x}_4 \oplus x_1 x_2 x_3 x_4$;

$f_2 = \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 \bar{x}_3 x_4 \oplus x_1 \bar{x}_2 x_3 x_4 \oplus x_1 x_2 x_3 \bar{x}_4$.

According $n = 4 < m = 6$ to this one-valued correspondence truth test

	0
	3
	8
	9
	6
	3

ISSN NO: 2770-4491
Date of Publication:20-12-2022

	3
	6
	4
0	5
1	8
2	3
3	
4	3
5	6

its $f(x_1, x_2, x_3, x_4) = (f_1, f_2, f_3, f_4, f_5, f_6)$ boolean function model would be:

$f_1 = \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 x_3 \bar{x}_4 \oplus x_1 \bar{x}_2 x_3 x_4 \oplus x_1 x_2 \bar{x}_3 \bar{x}_4 \oplus x_1 x_2 x_3 x_4$;

$f_2 = \bar{x}_1 \bar{x}_2 x_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 \bar{x}_3 x_4 \oplus x_1 \bar{x}_2 x_3 x_4 \oplus x_1 x_2 x_3 \bar{x}_4$;

$f_3 = \bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus \bar{x}_1 x_2 x_3 x_4 \oplus x_1 \bar{x}_2 \bar{x}_3 x_4 \oplus x_1 x_2 \bar{x}_3 \bar{x}_4$;

$f_4 = \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus \bar{x}_1 x_2 x_3 \bar{x}_4 \oplus x_1 x_2 \bar{x}_3 x_4 \oplus x_1 x_2 x_3 \bar{x}_4 \oplus x_1 x_2 x_3 x_4$;

$f_5 = \bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 x_3 \bar{x}_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus x_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus x_1 \bar{x}_2 x_3 \bar{x}_4 \oplus x_1 \bar{x}_2 \bar{x}_3 x_4 \oplus x_1 x_2 x_3 \bar{x}_4$;

$f_6 = \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_1 \bar{x}_2 x_3 x_4 \oplus \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_1 x_2 \bar{x}_3 x_4 \oplus x_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus x_1 \bar{x}_2 x_3 \bar{x}_4 \oplus x_1 x_2 \bar{x}_3 \bar{x}_4 \oplus x_1 x_2 x_3 \bar{x}_4$.

Looking at truth tables and $f_i (i = 1,2,3,4,5,6)$ function expressions, the following properties can be observed:

1. $n = m = 4$ when the numbers from 0 to 15 are matched with the same numbers with a mixed single value, that is, the condition of non- *linearity is* fulfilled;

2. $f_j (j = 1,2,3,4,5,6)$ number of " $2^4 : 2 = 2^3 = 8$ and " 1"in the column is 10, which means that the condition of 0"*balance* (*regularity) has been fulfilled* for these functions ;

3. $f_j (j = 1,2,3,4,5,6)$-expressions of functions $2^4 : 2 = 2^3 = 8$ contain parameters that are not identical to each other. This dissimilarity is a $2^4 : 2 = 2^3 = 8$ *sufficient condition to* ensure a one-valued match ;

4. If $n = m = 4$ - in the expression of the functions $2^4 : 2 = 2^3 = 8$, $f_j (j = 1,2,3,4,5,6)$ dissimilar terms less than t are involved, the one-value correspondence is violated, that is, the level of *nonlinearity decreases.*

By direct computations $n = 2^k, k = 2,3,..., N < \infty$ it is possible to ensure that properties 1-4 are preserved even when optional. Using these conclusions, it is $n (n = 4, 8, 16, 32, 64, 128, \ldots < \infty)$ possible to create a rule for building a Boolean function model that, in general, assigns a one-valued match to a mixture of numbers $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_n)$ from 0 to 1 without relying on a truth table . $2^n - 1$ That is, each of the components of such a one-valued compatibility function is represented by the XOR operation f_j

ISSN NO: 2770-4491
Date of Publication:20-12-2022

of all $x_i (i = 1, 2, \ldots, n)$ the variables themselves or the $2^n : 2 = 2^{n-1}$ pairs of dissimilar values, consisting of the conjunction of their negations $\oplus$, as follows:

$$f_j = x_1^{(1)}(j) \ldots x_n^{(1)}(j) \oplus x_1^{(2)}(j) \ldots x_k^{(2)}(j) \ldots x_n^{(2)}(j) \oplus \ldots \oplus x_1^{(2n-1)}(j) \ldots x_n^{(2n-1)}(j) \qquad (2)$$

where j =1, … n ; $1 \le k \le n$; $x_k^{(t)}(j) \in \{x_k, \bar{x}_k\} \left(1 \le t \le 2^{n-1}\right)$ consists of columns defined by boolean functions of the form. 2^{n-1} participation of terms less than , leads to violation of one-valued fit.

When we are above $n = m$-bul $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_n)$ function f_j-components, where j =1, ... n ; $(x_1, x_2, \ldots, x_n)$- to all values $(f_1, f_2, \ldots, f_n)$ of vectors - we have found the sufficiency condition for the method of determining matching to different values of vectors.

In conclusion, the following should be noted:

1) These obtained results are also of fundamental importance in the field of discrete mathematics.

2) It has a wide and promising application in building crypto-resistant reflections and creating crypto-algorithms.

3) Existing crypto-algorithms provide effective results in creating hardware devices.

any l of $(1 \le l \le 2^{n-1} - 1)$ 4) is 2^{n-1} involved allows to create new cryptanalysis methods and solve cryptanalysis problems with them.

5) can also be used in the construction of *bent functions* used in the solution of cryptographic tolerance problems .

6) 2^{n-1} there is no doubt that the study of the laws of the participation of many khads and finding the methods of their application will have an effective impact on the development of cryptography.

References

1. Akbarov D. E., Kamalov M.E., Musaev A. I. One The alphanumeric (plain) substitution encryption algorithm reflects the efficient use of boolean functions in hardware devices. //Newsletter of Tashkent Technical University. 2011, No. 3
2. Akbarov D. E., Kamalov M.E., Musaev A. I. // A multi-alphanumeric substitution encryption algorithm reflects efficient implementation of boolean functions in hardware devices. // Bulletin of Tashkent Technical University. 2011
3. Moldovyan N. A., Moldovyan A. A., Eremeev M. A. Cryptography: ot primitivov k sintezu algoritmov. -S Pb.: BXV-Peterburg, 2004. - 448 p .
4. Akbarov D.E. Cryptographic methods of ensuring information security and their application - Tashkent, "Mark of Uzbekistan", 2009 - 434 pages.
5. Sabirov Sh.O. Prilozhenie svoystva boovoy funktsii k resheniyu zadachi otsenka stoikosti preobrazovanii cryptographicheskikh algoritmov.
6. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. Basic cryptography: Uchebnoe posobie, 2-e izd. -M.: Helios ARV, 2002.-480 p.
7. Schneier B. Applied cryptography. Protocol , algorithm , text and language . - M.: publishing house TRIUMF, 2003 - 816 p.
8. Хонбобоев, Хакимжон Икромович, and Дилшод Улугбекович Султанов. "РУКОВОДСТВО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТЬЮ СТУДЕНТОВ ПРИ ОБУЧЕНИИ ПРЕДМЕТАМ ИНФОРМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ." Актуальные научные исследования в современном мире 12-1 (2016): 63-65.
9. Хонбобоев, Хакимжон Октамович, Мубина Хакимжоновна Икромова, and Мухаммад-Анасхон Хакимжонович Икромов. "Ta'limda axborot texnologiyalarni qollashning oziga xos xususiyatlari." Молодой ученый 3-1 (2016): 21-22.
10. Shukhratovich, Shirinov Feruzjon. "The Field of Computer Graphics and Its Importance, Role and Place in The Information Society." Texas Journal of Multidisciplinary Studies 4 (2022): 86-88.
11. Marufovich, Aripov Masud, and Shirinov Feruzjon Shuxratovich. "BO 'LAJAK INFORMATIKA FANI O 'QITUVCHILARINING GRAFIK AXBOROTLAR BILAN ISHLASH

ISSN NO: 2770-4491
Date of Publication:20-12-2022

KOMPETENSIYASINI RIVOJLANTIRISH." TA'LIM VA RIVOJLANISH TAHLILI ONLAYN ILMIY JURNALI 2.1 (2022): 183-187.
12. Хайдарова, Сапияхон. "Создание SQL-запросов в реляционных базах данных." Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика 3 (2020): 8-19.
13. Siddiqov, I. M. "THE IMPORTANCE OF USING THE ACT IN THE PROCESS OF DEVELOPMENT OF PRESCHOOL CHILDREN." Экономика и социум 5-1 (2021): 458-461.
14. Muydinovich R. I. et al. INFORMATIKA FANI YO ‘NALISHIDA ZAMONAVIY DASTURLASH TILLARINI O ‘RGANISHNING AHAMIYATI //INTERNATIONAL SCIENTIFIC RESEARCH CONFERENCE. – 2022. – Т. 1. – №. 4. – С. 75-78.
15. Marufovich, Aripov Masud. "INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANIDAN ELEKTRON O ‘QUV DARSLIKLAR YARATISHDA AUTOPLAY DASTURIDAN FOYDALANISH." BARQARORLIK VA YETAKCHI TADQIQOTLAR ONLAYN ILMIY JURNALI 2.3 (2022): 143-147.
16. Normatov, R. N., M. M. Aripov, and I. M. Siddikov. "Analysis Method of Structural-complex System Indicators by Decomposition Into Subsystems." JournalNX 7.04 (2021): 68-71.
17. O‘Ktam, O., Li Jumanqo‘Ziyev, and Islombek To‘Lqinjon O‘G‘Li. "MAKTAB O ‘QUVCHILARINING AXBOROT MADANIYATINI SHAKLLANTIRISHNING ASOSIY QONUNLARI VA TAMOYILLARI." Academic research in educational sciences 2.CSPI conference 1 (2021): 1073-1077.
18. Жуманкузиев, Уктамжон, and Уткир Йулдошев. "Подходы обучения языкам программирования в общеобразовательных школах." Общество и инновации 2.5/S (2021): 344-350.
19. Mamadjanova, S. V. "DESIGN FEATURES OF VIRTUAL LEARNING ENVIRONMENTS." European International Journal of Multidisciplinary Research and Management Studies 2.06 (2022): 1-5.
20. Xakimova, Yo T., I. I. Djurayev, and S. V. Mamadjonova. "INFORMATICS AND INFORMATION IN PRESCHOOL INSTITUTIONS METHODOLOGICAL SYSTEM OF INTRODUCTION OF SCIENCE “TECHNOLOGY”." Oriental renaissance: Innovative, educational, natural and social sciences 1.3 (2021): 105-110.
21. Juraev, Muzaffarjon Mansurjonovich. "PROSPECTS FOR THE DEVELOPMENT OF PROFESSIONAL TRAINING OF STUDENTS OF PROFESSIONAL EDUCATIONAL INSTITUTIONS USING ELECTRONIC EDUCATIONAL RESOURCES IN THE ENVIRONMENT OF DIGITAL TRANSFORMATION." Academicia Globe: Inderscience Research 3.10 (2022): 158-162.
22. Toshpulatov, Raximjon I. "MODERN METHODS AND TENDENCIES IN TEACHING INFORMATION TECHNOLOGY." International Journal of Pedagogics 2.09 (2022): 43-46.
23. Juraev, M. M. (2022). The value of open mass competitions in the process of digitalization of extracurricular activities of schoolchildren. Web of Scientist: International Scientific Research Journal, 3(10), 338-344.