E-commerce changed the way travel providers and online travel agencies (OTAs) served consumers. The 1960s launch of SABRE, the world's first computerized airline reservation system, led to the 1996 release of travel e-commerce website Travelocity. Today, online sales and travel e-commerce websites contribute to 66% of the revenue brought in by the global travel and tourism market. Altogether, the global market size of e-commerce travel exceeds $517.8 billion. Headless commerce allows travel e-commerce websites to continually innovate and respond to customers' changing needs, especially as the industry responds to the COVID-19 pandemic. By using headless CMS solutions, the best travel e-commerce websites may continue to iterate, innovate, and grow their market share.

References:

1. International Journal of Electronic Commerce
2. Fabricblog.com
3. Cofes.com
4. Webyurt.com
5. pinnacle-advisory.com

DOI https://doi.org/10.30525/978-9934-26-277-7-238

MATHEMATICAL CHARACTERISTICS OF BOOLEAN FUNCTIONS' MODELS IN CRYPTOGRAPHIC TRANSFORMATIONS

Umarov Sh. A.
Senior Teacher at the Department of Information Technology
Fergana branch of the Tashkent University
of Information Technologies
named after Muhammad al-Khwarizmi
Ferghana, Uzbekistan

Currently, in information exchange via a modern information and communication network, data is processed in accordance with digital codes and technological packages, technical and technological means. The main technical and technological means of digital processing, and the use of information, are mainly formed by transformations of Boolean functions.

Papers [1; 2] are devoted to the study of the features and properties of logical operations. Some features and properties of logical operations have been generalized to transformations of table replacement of bit connections [3–6].

This article explores the general mathematical characteristics of Boolean functions' models of logical operations and table replacement in applications of cryptographic and other transformations in the form of a Zhegalkin polynomial.

Here are some formalizations from primary sources [7; 8]. A block of bits $x = (x_1, x_2, ..., x_n)$ is considered as space elements $GF(2^n) = \{x = (x_1, x_2, ..., x_n) \in X\}$, $x_i \in \{0;1\}$. Let this block with some operation or a sequence of a limited number of some operations be transformed into elements of another space $GF(2^m) = \{y = (y_1, y_2, ..., y_m) \in Y : y_i \in \{0;1\}\}$ and this is expressed by Boolean functions in the following form:

$$Y = f(X) : GF(2^n) \to GF(2^m) \quad (1)$$

Such a transformation in vector form is represented by $f(x) = \{f_1(x), f_2(x), ..., f_m(x)\}$, $x_i, y_i \in GF(2)$, $x_i, y_i = \{0;1\}$.

The validity of this statement follows from the one-to-one property of transformations. In general, according to a logical operation $x * y = z$, where the variables take two different values "0" and "1", and the values are determined by 4 (four) pairwise different states of the values of the variables X and Y. These statements can be represented in the form of the following table, which is called the truth table:

$x * y$	0	1
0	z_{00}	z_{01}
1	z_{10}	z_{11}

where $z_{ij} \in \{0;1\}, i = 0.1;\ j = 0,1.$ Here, the variables z_{ij} take on two different values "0" and "1". According to this truth table, the Zhegalkin polynomial is modeled, expressing it analytically. To do this, we will use the universal rule. The column *z* contains elements with the values "1" and the members of the Zhegalkin polynomial are formed from the corresponding rows of the input blocks. In this case, the bit with "1" value is

assigned the variable itself or, and the bit with the value "0" is assigned the negation of the variable x or y. Thus, the model of the Zhegalkin polynomial corresponding to the truth table of this example looks as follows:

$$z = \bar{x}y \oplus x\bar{y}. \quad (2)$$

Using the proposed general rule, it's possible to model other logical operations introduced in [1-3].

Theorem 1. *Let some logical operation* *****-*** *be defined over the variables x and y, that is* $x * y = z$*, where* $x, y, z \in \{0,1\}$*. Suppose that in the truth table of this logical operation in the column z, not all values are "0" or not all values are "1", i.e. this operation is not the same as a "0" or "1" value.*

Now we turn to analytical modeling in the form of the Zhegalkin polynomial of the transformation of a table replacement by its truth table. First, we look at table swap conversions with two bit connections:

In general

x / y	00	01	10	11
00	z_{00}	z_{01}	z_{02}	z_{03}
01	z_{10}	z_{11}	z_{12}	z_{13}
10	z_{20}	z_{21}	z_{22}	z_{23}
11	z_{30}	z_{31}	z_{32}	z_{33}

As an example

x / y	00	01	10	11
00	11	10	01	00
01	10	01	00	11
10	01	00	11	10
11	00	11	10	01

Note that the input blocks of the truth table are formed by four bits from bit connections in two bits: $x=(x_1, x_2)$ and $y=(y_1, y_2)$. And output blocks in two bits – from bit connections in two bits: $z=(z_1, z_2)$. Column elements of input blocks take values from "0" to "15". And the elements of the column of the output blocks take values from "0" to "3", while these values are repeated four times. Proceeding as in the analytical modeling of the truth table of logical operations in the form of a Zhegalkin polynomial, the Zhegalkin polynomials are modeled for columns and accordingly:

$$z_1 = \bar{x}_1\bar{x}_2\bar{y}_1\bar{y}_2 \oplus \bar{x}_1\bar{x}_2\bar{y}_1 y_2 \oplus \bar{x}_1 x_2 \bar{y}_1\bar{y}_2 \oplus \bar{x}_1 x_2 y_1 y_2 \oplus$$
$$\oplus x_1\bar{x}_2 y_1\bar{y}_2 \oplus x_1\bar{x}_2 y_1 y_2 \oplus x_1 x_2\bar{y}_1 y_2 \oplus x_1 x_2 y_1\bar{y}_2 \quad (3)$$

and

$$z_2 = \bar{x}_1\bar{x}_2\bar{y}_1\bar{y}_2 \oplus \bar{x}_1\bar{x}_2y_1\bar{y}_2 \oplus \bar{x}_1x_2\bar{y}_1y_2 \oplus \bar{x}_1x_2y_1y_2 \oplus$$
$$\oplus x_1\bar{x}_2\bar{y}_1\bar{y}_2 \oplus x_1\bar{x}_2y_1\bar{y}_2 \oplus x_1x_2\bar{y}_1y_2 \oplus x_1x_2y_1y_2 \quad (4)$$

By formulas (3) and (4) by direct calculation, i.e. sequentially setting the values of the input blocks: (0000) 2 = 010, (0001) 2 = 110, (0010) 2 = 210, ..., (1111) 10 = 1510, performing the calculation, we obtain the corresponding output blocks of the truth table of the given example.

Definition 1. *If in the truth table of a table replacement the values* $0 \le z_{ij} = (z_{ij})_{10} \le 2^m - 1$ *are distributed and equal (by 2m times) or unequal, then they are respectively called uniformly distributed or unevenly distributed (regular or irregular) transformations of the table replacement.*

If we pay attention to the truth table of the transformation of logical operations and table replacement, the concatenation of blocks $x = (x_1x_2...x_m)$ and $y = (y_1y_2...y_m)$ is taken as an input block, i.e., $xy = (x_1x_2...x_my_1y_2...y_m)$. And blocks $z = (z_1z_2...z_m)$ are taken as an output block. The following conclusions take place:

1) If we assume that the block $x = (x_1x_2...x_m)$ represents part of the bits of the open message, and the block $y = (y_1y_2...y_m)$ represents part of the key bits of a certain length, in addition, the block $z = (z_1z_2...z_m)$ represents part of the bits of the encrypted message, then the table replacement truth table expresses the encryption rule table;

2) If we assume that the blocks $x = (x_1x_2...x_m)$ and $y = (y_1y_2...y_m)$ represent parts of the bits of the message being hashed, and the block $z = (z_1z_2...z_m)$ represents the hash result of these blocks, then the table replacement truth table expresses the rule without key hashing or information compression.

References:

1. Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions // *Прикладная дискретная математика.* 2018. №. 40. С. 23–33.

2. Akbarov D., Abdukadirov A., Umarov S. Research of general mathematical characteristics of logical operations and table replacements in

cryptographic transformations // *AIP Conference Proceedings.* – AIP Publishing LLC, 2022. Т. 2432. №. 1. С. 060020.

3. Poti P., Antinucci F. Logical operations // *Cognitive structure and development in nonhuman primates.* Psychology Press, 2019. С. 189–228.

4. Umarov S. A. Research on General Mathematical Characteristics of Boolean Functions' Models and Their Logical Operations and Table Replacement in Cryptographic Transformations // *Journal of Optoelectronics Laser.* 2022. Т. 41. №. 10. С. 126–133.

5. Акбаров Д. Е., Умаров Ш. А. Алгоритм хеш-функции с новыми базовыми преобразованиями // *Вісник Національного технічного університету України "Київський політехнічний інститут". Серія : Приладобудування.* 2016. № 51(1). С. 100–108. DOI: https://doi.org/10.20535/1970.51(1).2016.78112

6. Акбаров Д. Е., Умаров Ш. А. Новый алгоритм блочного шифрования данных с симметричным ключом // *Вісник Національного технічного університету України "Київський політехнічний інститут". Серія : Приладобудування.* 2016. № 52(2). С. 82–91. DOI: https://doi.org/10.20535/1970.52(2).2016.92963

7. Молдавян А. А., Молдавян Н. А. Криптография от примитивов к синтезу алгоритмов. СПб. : БХВ – Петербург, 2004, 448 с.

8. Молдавян А. А., Молдавян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. СПб. : БХВ – Петербург, 2004, 496 с.