Research on General Mathematical Characteristics of Boolean Functions’ Models and their Logical Operations and Table Replacement in Cryptographic Transformations

D.E. Akbarov¹, O. E. Kushmatov², Sh. A. Umarov², B. I. Bozarov³, M.Q. Abduolimova³

¹Doc.physical-mat. Sci., Kokand SPI, Kakand, Uzbekistan
²Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
³Fergana, Uzbekistan, Ferghana Polytechnic institute, Fergana, Uzbekistan

Abstract:
This given article inquires general mathematical characteristics of models of Boolean functions’ logical operations and table replacement. A rule is proposed for modeling the analytical model of the truth table in the form of a Zhegalkin polynomial. It is universal and it allows widespread effective use of it in the development of hardware-software and software cryptographic information security tools. In addition, the generality of the proposed rule will provide a broad effective application in the field of automation and control of processes with digital technologies and tools.

Introduction
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 [1-7] 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 [1-7].

Formulation
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.

Solution
Here are some formalizations from primary sources [8,9]. A block of bits \( x = (x_1, x_2, \ldots, x_n) \) is considered as space elements \( GF(2^n) = \{ x = (x_1, x_2, \ldots, x_n) \in X : x_i \in \{0;1\} \} \). Let this block with some operation or a sequence of a limited number of some operations be transformed into elements of another space \( GF(2^m) = \{ y = (y_1, y_2, \ldots, y_m) \in Y : y_i \in \{0;1\} \} \) and this is expressed by Boolean functions in the following form:

\[
Y = f(X) : GF(2^n) \rightarrow GF(2^m)
\]

Such a transformation in vector form is represented by

\[
f(x) = \{ f_1(x), f_2(x), \ldots, f_m(x) \}, \quad x_i, y_i \in GF(2), \quad x_i, y_i = \{0;1\}.
\]

To ensure a compact, convenient and efficient development of equipment and technology for digital information processing, the Boolean functions’ transformation of the table replacement are modeled [8-17] (Table 1.)

<table>
<thead>
<tr>
<th>x1x2…xn-1xn</th>
<th>f1 f2 … fm-1 fm</th>
</tr>
</thead>
<tbody>
<tr>
<td>0= 00 … 00</td>
<td>S0=s1(0)s2 (0)...sm-1(0)sm(0)</td>
</tr>
<tr>
<td>1= 00 … 01</td>
<td>S1=s1(1)s2 (1)...sm-1(1)sm(1)</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>2n -2 =11 … 10</td>
<td>S2n-2 =s1(2n-2 )s2 (2n-2 ) ... sm-1(2n-2 )sm(2n-2 )</td>
</tr>
<tr>
<td>2n -1 =11 … 11</td>
<td>S2n-1 =s1(2n-1 )s2 (2n-1 ) ... sm-1(2n-1 )sm(2n-1 )</td>
</tr>
</tbody>
</table>

Let the number of input bits \( n \) and output bits \( m \) be equal, i.e., in addition, the conditions are fulfilled in pairs, then function (1) has the inverse function

\[
X = f^{-1}(Y) : GF(2^m) \rightarrow GF(2^n).
\]

The validity of this statement follows from the one-to-one property of transformations [10]. In general, according to a logical operation \( x \ast y = z \), 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:

<table>
<thead>
<tr>
<th>( x \ast y )</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( z_{00} )</td>
<td>( z_{01} )</td>
</tr>
<tr>
<td>1</td>
<td>( z_{10} )</td>
<td>( z_{11} )</td>
</tr>
</tbody>
</table>

where \( z_{ij} \in \{0;1\}, \quad i = 0.1; \quad j = 0.1 \). Here, the variables \( z_{ij} \) take on two different values "0" and "1". The truth table can still be presented in the following form as table 1., i.e.

<table>
<thead>
<tr>
<th>( x ) ( y )</th>
<th>( z )</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>( z_{00} )</td>
</tr>
<tr>
<td>01</td>
<td>( z_{01} )</td>
</tr>
<tr>
<td>10</td>
<td>( z_{10} )</td>
</tr>
</tbody>
</table>
where $z_{ij} \in \{0; 1\}$, $i = 0.1; j = 0.1$.

As an example, the logical operation $\oplus$—XOR with the corresponding truth table, often effectively used in cryptographic and other transformations, is considered:

```
<table>
<thead>
<tr>
<th>x y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
</tr>
</tbody>
</table>
```

According to this truth table, the Zhegalkin polynomial is modeled, expressing it analytically [18-26]. 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:

$$z = \bar{x} y \oplus x \bar{y}.$$  (3)

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 $x \ast y = z$, 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 As an example

```
<table>
<thead>
<tr>
<th>x \ y</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>$z_{00}$</td>
<td>$z_{01}$</td>
<td>$z_{02}$</td>
<td>$z_{03}$</td>
</tr>
<tr>
<td>01</td>
<td>$z_{10}$</td>
<td>$z_{11}$</td>
<td>$z_{12}$</td>
<td>$z_{13}$</td>
</tr>
<tr>
<td>10</td>
<td>$z_{20}$</td>
<td>$z_{21}$</td>
<td>$z_{22}$</td>
<td>$z_{23}$</td>
</tr>
<tr>
<td>11</td>
<td>$z_{30}$</td>
<td>$z_{31}$</td>
<td>$z_{32}$</td>
<td>$z_{33}$</td>
</tr>
</tbody>
</table>
```

where $z_{ij} \in \{00; 01; 10; 11\}$, $i = 0,1,2,3; j = 0,1,2,3$.

Similarly as above, this table can be rewritten as follows:

In general As an example

```
\begin{array}{ccc|ccc}
\hline
x & y & z & x & y & z \\
\hline
00 & 00 & $z_{00}$ & 00 & 00 & 11 \\
\hline
\end{array}
```
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:

\[
\begin{align*}
\bar{z}_1 &= \bar{x}_1 \bar{x}_2 \bar{y}_1 \bar{y}_2 \oplus \bar{x}_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 \bar{y}_2 \oplus x_1 x_2 \bar{y}_1 y_2 \\
\oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \\
\end{align*}
\]

(4)

and

\[
\begin{align*}
\bar{z}_2 &= \bar{x}_1 \bar{x}_2 \bar{y}_1 \bar{y}_2 \oplus \bar{x}_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 \bar{y}_2 \oplus x_1 x_2 \bar{y}_1 y_2 \\
\oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \oplus x_1 x_2 y_1 y_2 \\
\end{align*}
\]

(5)

By formulas (4) and (5) by direct calculation, i.e. sequentially setting the values of the input blocks: \( (0000)_2 = 010 \), \( (0001)_2 = 110 \), \( (0010)_2 = 210 \), ..., \( (1111)_2 = 1510 \), performing the calculation, we obtain the corresponding output blocks of the truth table of the given example. Obviously, the method of mathematical induction can be used to prove this rule also holds for the general case, that is, it is true in the case of \( n \) - inputs and \( m \) - outputs, where, for example, such table replacement transformations can be provided in the following form (table 2):

<table>
<thead>
<tr>
<th>( x ) / ( y )</th>
<th>( y_0 )</th>
<th>( y_1 )</th>
<th>( \ldots )</th>
<th>( y_i )</th>
<th>( \ldots )</th>
<th>( y_{2^n - 1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_0 )</td>
<td>( z_{00} )</td>
<td>( z_{01} )</td>
<td>( \ldots )</td>
<td>( z_{0i} )</td>
<td>( \ldots )</td>
<td>( z_{0,2^n - 1} )</td>
</tr>
<tr>
<td>( x_1 )</td>
<td>( z_{10} )</td>
<td>( z_{11} )</td>
<td>( \ldots )</td>
<td>( z_{1i} )</td>
<td>( \ldots )</td>
<td>( z_{1,2^n - 1} )</td>
</tr>
</tbody>
</table>
If the length of the block of connecting bits is \( m = 2 \) bits, then the number of different such blocks is equal \( 2^m = 2^2 = 4 \), that is: 00, 01, 10, 11.

In the case of \( m = 3 \) bits and there are \( 2^m = 2^3 = 8 \) places, respectively: 000, 001, 010, 011, 100, 101, 110, 111.

Similarly, in the case of \( m = 4 \) and \( 2^m = 2^4 = 16 \), and so on.

The size of the table expressing the results \( m \times m \) table replacements, the numerical values \( z_{ij} = \left( z_{ij0} z_{ij1} \ldots z_{ij2^m-1} \right)_2 \) satisfy the condition \( 0 \leq z_{ij} = \left( z_{ij0} \right)_{10} \leq 2^m - 1 \), the \( m \)-bit length conversion result \( z \) performed on the \( m \)-bit blocks the bit \( x \) and \( y \) is not changed. In this case, the length of the input block "xy" transformation replacement tables equal to \( 2m \), and the length of output blocks "\( z_{ij} \)" equals \( m \).

**Definition 1.** If in the truth table of a table replacement the values \( 0 \leq z_{ij} = \left( z_{ij0} \right)_{10} \leq 2^m - 1 \) 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.

Similarly, as above, this table can be rewritten as follows:

In general As an example

<table>
<thead>
<tr>
<th>( X_i )</th>
<th>( x )</th>
<th>( z_{ij0} )</th>
<th>( z_{ij} )</th>
<th>( x )</th>
<th>( z_{ij0} )</th>
<th>( z_{ij} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_{2^n-1} )</td>
<td>( z_{2^n-1,0} )</td>
<td>( z_{2^n-1,1} )</td>
<td>( \ldots )</td>
<td>( z_{2^n-1,i} )</td>
<td>( \ldots )</td>
<td>( z_{2^n-1,2^n-1} )</td>
</tr>
</tbody>
</table>

Where each value \( z_{ij} \) on the column \( z \) is repeated exactly \( 2^m \) times, i.e., truth table by regular property or not all values \( z_{ij} = \text{const} \in \{0,1,\ldots,2^m-1\} \), i.e., this transformation is not identical.

Let’s present the following generalized transformation theorem for table replacement, as in the case of transformation using logical operations.

**Theorem 2.** Let the transformation of the table replacement be defined over the variables \( x = (x_1 x_2 \ldots x_m) \) and \( y = (y_1 y_2 \ldots y_m) \), that is \( xy = (x_1 x_2 \ldots x_m y_1 y_2 \ldots y_m) = (z_1 z_2 \ldots z_m) = z \), where \( x, y, z \in \{0,1,\ldots,2^m-1\} \). Suppose that not all values \( z_{ij} = \text{const} \in \{0,1,\ldots,2^m-1\} \) are in the truth table of the table replacement transformation, i.e., this transformation is not identical. Then the analytical model of the truth table in the form of a Zhegalkin...
polynomial is formed as follows: in the column $z_i$, where $0 \leq i \leq m$ the output blocks $z = (z_1, ..., z_m)$ contain elements with the values "1" and the members of the Zhegalkin polynomial are formed according to the corresponding rows of the input blocks $xy = (x_1, ..., x_m, y_1, ..., y_m)$ according to the rule that the bit with the "1" value is associated with the variable itself $x_i$ or $y_i$, and the bit with the value "0" is put into matching negation of a variable $\overline{x_i}$ or $\overline{y_i}$.

According to the rule of assertion of the theorem, the analytical model of the truth table of the given example in the form of a Zhegalkin polynomial will look like:

$z_1 = \overline{x_1}x_2...x_m\overline{y_1}y_2...y_m \oplus \ldots \oplus x_1x_2...x_my_1y_2...y_m$,

$z_2 = x_1x_2...x_my_1y_2...y_m \oplus \ldots \oplus x_1x_2...x_my_1y_2...y_{m-1}y_m$,

$z_{m-2} = \overline{x_1}x_2...x_m\overline{y_1}y_2...y_m \oplus \ldots \oplus x_1x_2...x_my_1y_2...y_m$,

$z_{m-1} = x_1x_2...x_my_1y_2...y_m \oplus \overline{x_1}x_2...x_my_1y_2...y_m \oplus x_1x_2...x_my_1y_2...y_m$,

$z_m = x_1x_2...x_my_1y_2...y_m \oplus x_1x_2...x_my_1y_2...y_{m-1}y_m \oplus x_1x_2...x_my_1y_2...y_m$.

Now let’s briefly mention some theoretical and practical scientific results.

**Analysis of the obtained results.**

If we pay attention to the truth table of the transformation of logical operations and table replacement, the concatenation of blocks $x = (x_1, ..., x_m)$ and $y = (y_1, ..., y_m)$ is taken as an input block, i.e., $xy = (x_1, ..., x_m, y_1, ..., y_m)$. And blocks $z = (z_1, ..., z_m)$ are taken as an output block. The following conclusions take place:

1. If we assume that the block $x = (x_1, ..., x_m)$ represents part of the bits of the open message, and the block $y = (y_1, ..., y_m)$ represents part of the key bits of a certain length, in addition, the block $z = (z_1, ..., z_m)$ 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 $x = (x_1, ..., x_m)$ and $y = (y_1, ..., y_m)$ represent parts of the bits of the message being hashed, and the block $z = (z_1, ..., z_m)$ represents the hash result of these blocks, then the table replacement truth table expresses the rule without key hashing or information compression;

3. If we assume that the block $x = (x_1, ..., x_m)$ represents a part of the bits of an open message transmitted over the network of the information and communication network, and the block $y = (y_1, ..., y_m)$ represents a part of the error correction bits for reliable information transmission, then the table replacement truth table can express a coding table [11, 12] of information.

4. The proposed rule for modeling the analytical model of the truth table in the form of the Zhegalkin polynomial is universal and allows wide and effective use in the development of hardware-software and software cryptographic information security tools.
Note that to transform the discrete domain of definition of the argument value and change the value by the corresponding truth tables on the basis of the proposed rule, one can model their analytical model in the form of a Zhegalkin polynomial. This property will provide a broad effective application of the proposed rule in the field of automation and control of processes with digital technologies and tools.

Conclusion.

The obtained results in a compact mathematical form with the corresponding definitions, statements, their analysis express the fundamental foundations. Provides the basic foundations for the development of hardware-software and software cryptographic information security tools with broad effective applications.

REFERENCES.

11. Moldavian A. A., Moldavian N. A. Cryptography from primitives to the synthesis of algorithms. SPb.: BHV - Petersburg, 2004, 448 p


