ISSN: 2181-4171

# Engineering Problems and Innovations

Vol. 02 Iss. 04 || Dec 27th, 2024

Том - 02 | | Вып. - 04

Проблемы инженерии и Инновации



SCAN ME

Google Scholar INDEX COPERNICUS INTERNATIONAL zenodo Academic Resource Index ResearchBib

Fergana - 2024

**Главный редактор**

Зокиров Санжар Икромжон угли
д.ф.ф.-м.н., PhD

Журнал зарегистрирован 28 декабря 2022 года Агентством информации и массовых коммуникаций при Администрации Президента Республики Узбекистан

**Сертификат № 055940**
**ISSN 2181-4171**

**Языки издания**:
Русский, английский

**Председатель эксп. совета**

*Ф.М.Мухтаров - д.ф.т.н, PhD. директор ФФ ТУИТ*

**Ответственные редакторы разделов**

**Т.М.Абдуллаев**
*д.ф.т.н., PhD, ФФ ТУИТ*

**Н.И.Иброхимов**
*д.ф.ф.-м.н., PhD, ФФ ТУИТ*

**А.Р.Нурматов**
*PhD, д.ф.ист.н.,НамГУ*

**Г.А.Умарова**
*к.п.н., доц., АндМИ*

**Корректоры**

Порубай Оксана Витальевна
Лазарева Марина Викторовна
Обиджонов Зафаржон Одилжон угли

**Редакционная коллегия:**

**Б.К.Сарсенбаев -** *д.т.н, проф., акад., дейст. член Нац. Акад. Респ. Казахстан*
**В.Ю.Рудь** - *д.ф.-м.н., Физико-технический институт им. А.Ф.Иоффе, Санкт-Петербург, Россия*
**Н.Б.Бейсенханов** - *д.ф.-м..н., проф. АО "Казахстанско-Британский Технический Университет", Алматы, Казахстан*
**Б.Р.Исмаилов** - *д.т.н., проф. Южно-Казахстанский университет им. М. Ауэзова , Шымкент, Казахстан*
**А.В.Аржанников -** *д.ф.-м.н., Новосибирский государственный университет, Институт ядерной физики СО РАН, Новосибирск, Россия*
**А.М.Касимахунова -** *д.т.н., проф. ФерПИ, Фергана, Узбекистан*
**И.Бйорно -** *к.н.,PhD, Имеритус, Датский технический университет, Копенгаген, Дания*
**Л.К.Мамадалиева -** *д.т.н., проф. ФерПИ, Фергана, Узбекистан*
**Ж.Т.Айменов -** *д.т.н., проф. Южно-Казахстанский университет им.М.Ауезова, Шымкент, Казахстан*
**Х.Б.Исмаилов -** *к.т.н. доцент, Южно-Казахстанский университет им. М. Ауэзова , Шымкент, Казахстан*
**В.В.Краснощеков -** *к.т.н. Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Российская Федерация*
**М.Д.Шабданов -** *к.т.н. ОшТУ , Ош, Киргизстан*
**В.М.Голубова -** *к.псх.н. Ростовский институт (филиал) ВГУЮ (РПА Минюста России), Ростов-на-Дону, Россия*

**Коллегия экспертного совета**

**О.Х.Отакулов -** *к.т.н., доц. Ферганский филиал ТУИТ, Узбекистан*
**О.С.Райимжонова** - *д.ф.т.н., PhD, доц, Ферганский филиал ТУИТ, Узбекистан*
**Р.А.Нурдинова -** *д.ф.т.н., PhD, доц., Ферганский филиал ТУИТ, Узбекистан*
**М.Э.Юнусалиев -** *к.т.н., PhD, доц., ФерПИ, Узбекистан*
**М.И.Исмоилов** - *к.т.н., PhD, доц., ФерПИ, Узбекистан*
**М.Т.Халилов** - *к.т.н., доц., АндМИ, Узбекистан*
**Г.А.Дадамирзаева -** *д.ф.ист.н., PhD, доц., НамГУ, Узбекистан*
**И.Т.Тожибоев -** *к.ф.-м.-н., доц., ФерГУ, Узбекистан*
**А.Ш.Тухтабаев -** *д.ф.ист.н., PhD, доц., НамГУ, Узбекистан*
**И.М.Исакова** - *д.п.н. доц., ФерГУ, Узбекистан*
**М.М.Турдиматов** - *к.т.н, доц., Ферганский филиал ТУИТ, Узбекистан*
**Д.Ф.Тухтасинов -** *д.ф.пед.н., PhD, доц., Ферганский филиал ТУИТ, Узбекистан*
**Н.Д.Ботирова** - *д.ф.пед.н., PhD, доц., Ферганский филиал ТУИТ, Узбекистан*
**Ш.Ж.Холматов** - *к.ф.н., доц., Ферганский филиал ТУИТ, Узбекистан*
**З.Н.Хатамова** - *д.ф.ист.н., PhD, доц., Ферганский филиал ТУИТ, Узбекистан*

**When using journal materials, you must indicate the source.**
**The authors of the articles are responsible for the content of the articles and for the very fact of their publication.**
**The editors do not always share the opinions of the authors and are not responsible for the unreliability of the published data.**
**The editorial board of the journal does not bear any responsibility to the authors and / or third parties and organizations for possible damage caused by the publication of the article.**

**Editor in chief**

Zokirov Sanjar
Ikromjon ugli
PhD in Phys. and Math. Sc.

The journal has been registered on December 28, 2022 by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan

**Certificate No. 055940**

**ISSN 2181-4171**

**Languages:**
Russian, English

**Chairman of exp. advice**
*F.M.Muxtarov - Ph.D. in tech. Sc., director of FB of TUIT*

**Responsible section editors**

**T.M.Abdullaev**
*PhD in Tech. Sc., FB of TUIT*

**N.I.Ibrokhimov**
*PhD in Phys. and Math. Sc., FB of TUIT*

**A.R.Nurmatov**
*Ph.D. in hist. sc., NamSU*

**G.A.Umarova**
*Cand. of ped. sc, assoc. prof., AndMI*

**Proofreaders**
Porubay Oksana Vitalevna
Lazareva Marina Viktorovna
Obidjonov Zafarjon Odiljon ugli

**Editorial board:**

**B.K.Sarsenbaev–** *Dr. of Tech. Sc., prof. Actual member of the National Acad. Rep. Kazakhstan*
**V.Yu.Rud'**– *Dr. of Phys. and Math. Sc., Ioffe Physicotechnical Institute, St.-Petersburg, Russia*
**N.B.Beisenkhanov**– *Dr. of Phys and Math. Sc. (Ds), full professor in Physics, JSC "Kazakh-British Technical University", Almaty, Kazakhstan*
**B.R.Ismailov**– *Dr. of Tech. Sc., prof., Mukhtar Auezov South Kazakhstan State University, Shymkent, Kazakhstan*
**A.V.Arzhannikov–** *Dr. of Sc. in Phys. and Math., prof., Novosibirsk St. University, Budker Institute of Nuclear Physics, Russian Federation*
**A.M.Kasimahunova** - *Dr. of Tech. Sc., prof., Fergana Polytechnic Institute. Fergana, Uzbekistan*
**I.Bjørnø -** *Assoc. Prof. PH.D, DTU imeritus, København, Denmark*
**L.K.Mamadaliyeva -** *Dr. of Tech. Sc., prof., Fergana Polytechnic Institute. Fergana, Uzbekistan*
**Zh.T.Aimenov–** *Dr. of Engineering (Ds), prof. Mukhtar Auezov South Kazakhstan State University, Shymkent, Kazakhstan*
**Kh.B.,Ismailov -** *PhD in Tech. Sc., Mukhtar Auezov South Kazakhstan State University, Shymkent, Kazakhstan*
**V.V.Krasnoshchekov -** *PhD in Engineering, Peter the Great St. Petersburg Polytechnic University, Russian Federation, St. Petersburg*
**M.D.Shabdanov–** *Can. of Tech. Sc., Osh Technological University, Osh, Kyrgyzstan*
**V.M.Golubova -** *PhD in Psych., Rostov Institute (branch) VGUYu (RPA of the Ministry of Justice of Russia) Russia, Rostov-on-Don*

**Expert Board**

**O.Kh.Otakulov**– *Cand. of tech. sc., assoc. prof., Fergana branch of TUIT, Uzbekistan*
**O.S.Raimzhonova** - *PhD, assoc. prof., Fergana branch of TUIT, Uzbekistan*
**R.A.Nurdinova -** *PhD, assoc. prof., Fergana branch of TUIT, Uzbekistan*
**E.M.Yunusaliev -** *Ph.D in Technics, assoc. prof., FerPI, Uzbekistan*
**M.M.Ismoilov** - *Cand. of tech. sc., PhD, assoc. prof., FerPI, Uzbekistan*
**M.T.Khalilov** - *Cand. of tech. sc., assoc. prof., AndMI, Uzbekistan*
**G.A.Dadamirzaeva -** *Ph.D in Hist. Sc., NamSU, Uzbekistan*
**I.T.Tojiboev -** *Cand. of Phys. and Math. Sc., assoc. prof., FerSU, Uzbekistan*
**A.Sh.Tukhtabaev -** *Ph.D in Hist. Sc., NamSU, Uzbekistan*
**M.T.Isakova** - *DSc in Psychology, FerSU, Uzbekistan*
**M.M.Turdimatov -** *Cand. of tech. sc., PhD, assoc. prof., Fergana branch of TUIT, Uzbekistan*
**D.F.Tukhtasinov** - *PhD on Ped., assoc. prof., Fergana branch of TUIT, Uzbekistan*
**N.D.Botirova** - *PhD on Ped., assoc. prof., Fergana branch of TUIT, Uzbekistan*
**Sh.J.Kholmatov** - *cand. phil., assoc. prof., Fergana branch of TUIT, Uzbekistan*
**N.Z.Khatamova** - *Ph.D in Hist. Sc., assoc. prof., Fergana branch of TUIT, Uzbekistan*

**When using journal materials, you must indicate the source.**
**The authors of the articles are responsible for the content of the articles and for the very fact of their publication.**
**The editors do not always share the opinions of the authors and are not responsible for the unreliability of the published data.**
**The editorial board of the journal does not bear any responsibility to the authors and / or third parties and organizations for possible damage caused by the publication of the article.**

# CONSTRUCTING BUL-FUNCTION MODELS BASED ON TRUTH TABLES FOR CRYPTOGRAPHICALLY STRONG

***Shukhratjon Umarov***

*Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi*
*Associate Professor of the Department of Information Security*

*e-mail: sh.umarov81@mail.ru*

***Abstract.*** *This article discusses methods for developing convenient and efficient cryptographic algorithms using truth tables. It describes methods for creating reflections using Boolean function models, their advantages and disadvantages, and methodologies for designing and using Boolean functions. This opens up opportunities for developing more reliable and efficient functions for cryptographically strong reflections.*

***Keywords:*** *Boolean function model, truth table, cryptography, discrete mathematics, combinatorial design, cryptographic algorithm, security, encryption*

# ПОСТРОЕНИЕ МОДЕЛЕЙ БУЛ-ФУНКЦИЙ НА ОСНОВЕ ТАБЛИЦ ИСТИННОСТИ ДЛЯ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ

***Шухратжон Умаров***

*Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий*
*Доцент кафедры информационной безопасности*
*sh.umarov81@mail.ru*

***Аннотация.*** *В данной статье рассматриваются методы разработки удобных и эффективных криптографических алгоритмов с использованием таблиц истинности. Описываются методы создания отражений с использованием моделей булевых функций, их преимущества и недостатки, а также методологии проектирования и использования булевых функций. Это открывает возможности для разработки более надежных и эффективных функций для криптографически стойких отражений.*

***Ключевые слова:*** *модель булевой функции, таблица истинности, криптография, дискретная математика, комбинаторное проектирование, криптографический алгоритм, безопасность, шифрование*

**Introduction.** In the security of modern cryptographic systems, cryptographic mirroring functions are important. These functions are used in data encryption and decryption processes and determine their complexity and level of cryptoresistance. Crypto-tolerant reflection function models are often based on discrete mathematics and combinatorial design principles. Knowing how to construct models of crypto-resistant mirror functions with the help of truth tables

and verify their security properties allows to create new crypto algorithms in this field. Truth tables are an important tool in the design of crypto-tolerant reflection function models, allowing the complete representation of functions and the precise specification of output values for each combination of their inputs.

Boolean functions of cryptographic representations can be modeled on the basis of their truth tables [1, 2]. It is said that the Boolean function of reflection can be built on the basis of the truth table, and the complexity of the construction method and process is emphasized [3]. In fact, the size of the truth table increases dramatically as the number of reflection variables increases. However, given a reflection truth table, a general method of constructing its boolean function is developed and shown to be uncomplicated.

**Materials and methods**

Let's say the number of reflection variables is n=4,8,16,32,64,128 and so on. In this article, a method has been created that allows you to build a Boolean function model based on the properties of the reflection itself and the conditions related to the cryptographic properties, without depending on the size of the truth table.

When the number of Boolean function variables is $n=4$ $(x_1, x_2, x_3, x_4)$, $x_i \in \{0;1\}$, then all possible values $\{0,0,0,0\}; \{0,0,0,1\}; \{0,0,1,0\}; \{0,0,1,1\}; \ldots, \{1,1,1,1\}$ corresponding to different states of this vector of variables are $0000=0;\ 0001=1;$ $0010=2;\ 0011=3; \ldots, 1111=15$ number $2^n=2^4=16$. $n=5$ at $2^5=32$, $n=6$ at $2^6=64$, $n=7$ at $2^7=128$, $n=8$ at $2^8=256$, $n=9$ at $2^9=512$ and so on. In general, if the number of variables is $n$, the set of all possible values of the $(x_1, x_2, ..., x_n)$-vector is $\{0;1;2;...;2^n-1\}$. Cryptographic algorithms use reflections with the number of variables as $n=16, 32, 64, 128$ [4].

For example, in the GOST 28147-89 healing algorithm

$$[k(32\ bit)+m(32\ bit)] \bmod 2^{32} = z(32\ bit) \qquad (1)$$

from mirroring, increasing bytes in the AES-FIPS 197 encryption algorithm

$$s(8\ bit)\cdot k(8\ bit)=n(8\ bit) \qquad (2)$$

reflections are used.

32-bit vectors $2^{32}$ corresponding to various 64-bit vectors in $2^{64}$ are used to construct the Boolean function of reflection (1) based on the addition operation on a finite field with characteristic $2^{32}$, based on its truth table.

This situation makes it difficult to model the corresponding Boolean function based on the truth table.

**Discussions and results**

Encryption algorithm mappings can generally be viewed as replacing $GF(2)^n = \{x = (x_1, x_2, ..., x_n) \in X : x_i \in \{0;1\}\}$ – space elements with other $GF(2)^m = \{y = (y_1, y_2, ..., y_m) \in Y : y_i \in \{0;1\}\}$ – space elements through a finite number of operations or sequences, and it is expressed in the form of functions as follows:

$$Y = f(X) \; ; \; GF(2)^n \to GF(2)^m .$$

The vector-function in this reflection expression is described in the form of this $f(x) = \{f_1(x), f_2(x), ..., f_m(x)\}$, here $x_i, y_i \in GF(2)$, ie $x_i, y_i = \{0;1\}$.

The so-called algebraic normal form for Boolean function expressions is as follows

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

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

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

Table 1.

$n = m = 4$ is the truth table

| | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 2 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 3 |
| 2 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 4 |
| 3 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 7 |
| 4 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 11 |
| 5 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 13 |
| 6 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 15 |
| 7 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 14 |
| 8 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 6 |
| 10 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 8 |
| 11 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 12 |
| 12 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 10 |
| 13 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 14 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 5 |
| 15 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 9 |

According to the truth table (Table 1) when $n=m=4$, its $f(x_1,x_2,x_3,x_4)=(f_1,f_2,f_3,f_4)$ boolean function model is as follows [5,6]:

$$f_1=\bar{x}_1x_2\bar{x}_3\bar{x}_4\oplus\bar{x}_1x_2\bar{x}_3x_4\oplus\ldots\oplus x_1x_2\bar{x}_3\bar{x}_4\oplus x_1x_2x_3x_4$$
$$f_2=\bar{x}_1\bar{x}_2x_3\bar{x}_4\oplus\bar{x}_1\bar{x}_2x_3x_4\oplus\ldots\oplus x_1\bar{x}_2x_3x_4\oplus x_1x_2x_3\bar{x}_4$$
$$f_3=\bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4\oplus\bar{x}_1\bar{x}_2\bar{x}_3x_4\oplus\ldots\oplus\bar{x}_1x_2x_3\bar{x}_4\oplus x_1x_2\bar{x}_3\bar{x}_4$$
$$f_4=\bar{x}_1\bar{x}_2\bar{x}_3x_4\oplus\bar{x}_1\bar{x}_2x_3x_4\oplus\ldots\oplus x_1x_2x_3\bar{x}_4\oplus x_1x_2x_3x_4.$$

Based on this, the following definition is introduced, which is directly related to the solutions of the researched problems.

**Definition.** If the number of bits of the input block is $n$ and the number of bits of the output block is $m$, n=m and the condition $S_i\neq S_j$ is fulfilled in pairs, then the representation expressed in (1) is called bijective-regular.

If we pay attention to the expressions of the truth table and the functions $f_i(i=1,2,3,4)$, the following properties are derived:

- The numbers from 0 to 15 are mixed single-valued matches of the same numbers, i.e. the condition of non-linearity is satisfied;

- $f_j(j=1,2,3,4)$ - the number of "0" and "1" in the column consists of $2^4:2=2^3=8$, which means that the condition of balance (regularity) is fulfilled for these;

- $f_j(j=1,2,3,4)$ - function expressions contain $2^4:2=2^3=8$ dissimilar values. This it $2^4:2=2^3=8$ dissimilarity is a sufficient condition to ensure a one-valued match;

- if the expressions of $f_j(j=1,2,3,4)$ - functions contain less than $2^4:2=2^3=8$ dissimilar terms, the one-valued correspondence is violated, that is, the level of nonlinearity decreases..

**Confirmation.** If the reflection (1) has $n=m$, and it is a bijective-regular reflection, then there is a reflection function (2) which is inverse to it, and the reciprocal one-valued property holds.

By direct computations, it is possible to ensure that these properties are preserved even in the case of optional $n=2^k, k=2,3,...,N<\infty$. As a result, it is possible to construct a $F=f(x_1,x_2,\ldots,x_n)=(f_1,f_2,\ldots,f_n)$ boolean function model that, in general, when $n(n=4,8,16,32,64,128,\ldots<\infty)$, sets a one-valued match to a mixture of the same numbers from 0 to $2^n-1$ without relying on the truth table.

Each of the $f_j$-components of such a one-valued compatibility function is represented by the $\oplus$ - XOR operation of $2^n:2=2^{n-1}$ (pairwise) dissimilar values

consisting of all $x_i (i = 1, 2, \ldots, n)$ variables themselves or the conjunction of their negations, as follows:

$$f_j = x_1^{(1)}(j) \ldots x_n^{(1)}(j) \oplus x_1^{(2)}(j) \ldots x_k^{(2)}(j) \ldots x_n^{(2)}(j) \oplus \ldots \oplus x_1^{(2n-1)}(j) \ldots x_n^{(2n-1)}(j) \qquad (3)$$

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

Above, we found the sufficiency condition for the method of determining $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_n)$-Boolean function $f_j$-components when $n = m$, corresponding to all values of $(x_1, x_2, \ldots, x_n)$-vectors and different values of $(f_1, f_2, \ldots, f_n)$-vectors in pairs, here $j = 1,...,n$.

In many cases, for example: in $S$-blocks of the DES encryption algorithm, in reflections based on the compression table [7], in hash-function algorithms, in reflections performed by performing algebraic operations based on permutations and substitutions that can be expressed by $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_m)$-Boolean functions satisfying the condition $n > m$ work will be done.

This is the way to determine the $f_j$-components of this function so that all values of the $(x_1, x_2, \ldots, x_n)$-vectors correspond to the repetition of some values of the $(f_1, f_2, \ldots, f_m)$-vectors, , here $j = 1,...,m$.

Even in the case of $n > m$, the $f_j$-components ( $j = 1,...,m$ ) are arbitrary or m chosen taking into account certain properties of the truth table, as in the case where $m$ is exactly $n = m$, each of which consists of the conjunction of all $x_i (i = 1, 2, \ldots, n)$ variables themselves or their negations $2^n : 2 = 2^{n-1}$ (pair -with a pair) is defined by Boolean functions of the form (3) expressed by the $\oplus$ - XOR operation of their dissimilar terms.

Such detection ensures non-linearity, regularity and non-decreasing degree of non-linearity [8].

Sometimes, for example, in the E-expansion tabular permutation of the DES encryption algorithm, permutations and permutations such as mapping an 8-bit number in the S-block of the Blowfish crypto-algorithm to a 32-bit number can be represented by an $F = f(x_1, x_2, \ldots, x_n) = (f_1, f_2, \ldots, f_m)$-Boolean function satisfying the condition $n < m$ [9]. In this case, the $f_j$-components ( $j = 1,...,n$ ) are arbitrary or selected taking into account certain properties of the truth table, as in

the case where n is exactly $n=m$, each of which consists of the conjugation of all $x_i(i=1,2,\ldots,n)$ variables themselves or their negations $2^n:2=2^{n-1}$ (in pairs) is determined by Boolean functions of the form (3) expressed by the XOR operation of their non-similar terms.

The number of pairs of $x_1^{(t)}\ldots x_k^{(t)}\ldots x_n^{(t)}$-terms made up of conjunctions is $2^n$, the number of terms of the expression of functions with $f_j$-components is $2^{n-1}$, and the number of different combinations made of $2^n$ elements from $2^{n-1}$ is calculated by this

$$C_{2^n}^{2^{n-1}}=\frac{(2^n)!}{(2^{n-1})!(2^n-2^{n-1})!}=\frac{(2^n)!}{(2^{n-1})!(2^{n-1})!}$$

expression. Here $1\le k\le n$; $x_k^{(t)}\in\{x_k,\bar{x}_k\}\left(1\le t\le 2^{n-1}\right)$.

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 $f_j$-components of the Boolean function $F=f(x_1,x_2,\ldots,x_n)=(f_1,f_2,\ldots,f_m)$ satisfying the condition $n<m$ according to the above requirements.

**Conclusion**

The definition of bijective-regularity is included in the general mathematical basis of constructing Boolean function models for digital reflection devices, constructing a forward and reverse Boolean function model when $n=m$ for input block bits $n$ and output block bits $m$, and matching output blocks to input blocks when $n\ge m$. The construction of this function model was expressed through assertion.

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 the construction of crypto-resistant reflections and creation of crypto-algorithms.

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

4) Studying the laws of violation of one-valued compatibility when any $l$ of $2^{n-1}$ participates in $(1\le l\le 2^{n-1}-1)$ makes it possible to create new cryptanalysis methods and solve cryptanalysis problems with them.

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

6) Studying the laws of participation of many numbers from $2^{n-1}$ and finding their application methods also effectively affects the development of cryptography.

**References:**

1. Akbarov, D. E. (2009). Cryptographic methods of ensuring information security and their application. Tashkent," Mark of Uzbekistan" publishing house, 432(2).
2. Umarov, S. A. (2022). Research on General Mathematical Characteristics of Boolean Functions’ Models and Their Logical Operations and Table Replacement in Cryptographic Transformations. Journal of Optoelectronics Laser, 41(10), 126-133.
3. Preneel, B., & Logachev, O. A. (Eds.). (2008). Boolean functions in cryptology and information security (Vol. 18). IOS Press.
4. Wu, C. K., & Feng, D. (2016). Boolean functions and their applications in cryptography.
5. Akbarov, D., & Abdukadirov, A. (2022, June). Research of general mathematical characteristics of logical operations and table replacements in cryptographic transformations. In AIP Conference Proceedings (Vol. 2432, No. 1). AIP Publishing.
6. Akbarov, D. E., & Umarov, S. A. (2021). Mathematical characteristics of application of logical operations and table substitution in cryptographic transformations. Scientific-technical journal, 4(2), 6-14.
7. Umarov, S. A. (2023). Mathematical characteristics of boolean functions’models in cryptographic transformations. Publishing House “Baltija Publishing”.
8. Tiwari, S., & Sharma, D. (2023). On higher order nonlinearities of Boolean functions. Cryptography and Communications, 15(4), 821-830.

Научно-технический журнал “Проблемы инженерии и Инновации”

Адрес редакции:
150100, Ферганская област, г. Фергана, улица Солим, дом 23/4, кв. 26

E-mail:
chief_editor@epai.uz

Наш сайт:
https://epai.uz/

Учредителем научно-технического журнала
**«Engineering problems and innovations»** является ООО “Fer-Teach”.
Журнал издается с 2023 года, зарегистрирован 28 декабря 2022 года Агентством информации и массовых коммуникаций при Администрации Президента Республики Узбекистан (Сертификат № 055940).

**ISSN: 2181-4171**.

«Инженерные проблемы и инновации» является специализированным журналом в области техники и охватывает все основные направления исследований и разработок в различных областях технических наук: физике, математике, информационных технологиях. В журнале также публикуются научные стати по лингвистике, методике преподавания и истории развития технических наук.

**Языки издания**: Русский, английский, узбекский