УДК 519.719.1, 681.322

Ткаченко В.Г., Синявский О.В.
Ткаченко В.Г., Сінявський О.В.
Tkachenco V.G., Sinyavsky.O.

ДЕРЕВЬЯ ТИПОВ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ И КРИПТОСИСТЕМЫ С БЛОКАМИ ПЕРЕМЕННОЙ ДЛИНЫ

ДЕРЕВА ТИПІВ МОНОТОННИХ БУЛЕВИХ ФУНКЦІЙ ТА КРИПТОСИСТЕМИ З БЛОКАМИ ЗМІННОЇ ДОВЖИНИ

TREES OF THE TYPES OF MONOTONOUS BOOLEAN FUNCTIONS AND CRYPTOSYSTEMS WITH THE BLOCKS OF THE VARIABLE LENGTH

Аннотация. В статье рассмотрена возможность применения типов монотонных булевых функций (МБФ) при построении криптосистемы, основанной на разбиении информации на блоки переменной длины. Доказана теорема об однозначном правом (левом) разложении любого типа МБФ. Операция сдвиг-суммы типов МБФ расширена на произвольные векторы и введены две новые операции: выделения максимальной правой части и выделения максимальной левой части. Это позволило получить удобный критерий: является ли произвольный вектор типом МБФ, а также получить дерево разложения любого типа МБФ на нулевые типы, левые (правые) единицы различных рангов. Эти деревья разложения имеют различное число вершин и используются для получения блоков зашифрованной информации переменной длины.

Анотація. У статті розглянута можливість застосування типів монотонних булевих функцій (МБФ) при побудові криптосистеми, заснованої на розбитті інформації на блоки змінної довжини. Доказана теорема про однозначне праве (ліве) розкладання будь-яких типів МБФ. Операція зсув-суми типів МБФ розширена на довільні вектори і введено дві нові операції: виділення максимальної правої частини і виділення максимальної лівої частини. Це дозволило отримати зручний критерій: чи є довільний вектор типом МБФ, а також отримати дерево розкладання будь-якого типу МБФ на нульові типи, ліві (праві) одиниці різних рангів. Ці дерева розкладання мають різне число вершин і використовуються для отримання блоків зашифрованої інформації змінної довжини.

Summary. In the article possibility of application of types of monotonous Boolean functions (MBF) is considered at the construction of cryptosystem, based on breaking up of information on the blocks of variable length. The theorem about the single-valued by right (left) decomposition of any type of MBF is proven.The operation of shift-sum types of MBF is extended on every vectors and two new operations are entered: excretions maximal right part and excretions maximal left part. It allowed to get a comfortable criterion whether there is an every vector by the type of MBF, and also to get the tree of decomposition of any type of MBF on zero types, left (right) units of different rank of type. These trees of decomposition have different number of nodes and are used for obtaining the blocks of encoded information of variable length.

В настоящее время передача цифровой информации в телекоммуникационных системах получила широкое распространение. В связи с этим возникает проблема повышения требований к обеспечению информационной безопасности.

Наиболее часто в настоящий момент используются асимметричные криптоалгоритмы или алгоритмы с открытым ключом. Но алгоритмы с закрытым ключом гораздо проще реализуются как программно, так и аппаратно и шифры с закрытым ключом работают быстрее шифров с открытым ключом. Также надежность алгоритмов с открытым ключом в настоящее время обоснована гораздо хуже, чем надежность алгоритмов с закрытым ключом. Поэтому для организации шифрованной связи в настоящее время применяются шифры с закрытым ключом, а новые методы применяются только там, где нельзя использовать симметричные криптоалгоритмы, т. е. для цифровой подписи или открытого распределения ключей. В настоящее время блочные шифры являются основой, на которой реализованы практически все криптосистемы (см. [1] … [5]). Все эти криптосистемы не разработаны для блоков информации переменной длины, а используют блоки постоянной длины. В [6] рассмотрены типы монотонных булевых функций (МБФ), которые удобно использовать для реализации криптосистемы с блоками переменной длины.

Однако в литературе шифрование на основе типов МБФ не описано.

Целью настоящей работы является построение криптосистем с блоками переменной длины за счёт использования деревьев разложения типов МБФ.

1. Основные понятия. Вектор $\tilde{a} = (a_n,...,a_i,...,a_1)$, компоненты которого принимают значения из множества $\{0,1\}$, будем называть входным набором булевой функции от *n* переменных. Множество всех таких входных наборов будем называть булевым кубом [3] ранга *n*. Сами входные наборы $\tilde{a}$ назовём вершинами булева куба. Любую булеву функцию можем определить множеством входных наборов булева куба, на которых эта функция равна единице. Расстоянием Хемминга [3] между двумя входными наборами $\tilde{a}$ и $\tilde{b}$ называется число $\rho(\tilde{a},\tilde{b})$, равное количеству компонент, в которых они различаются. Вершины $\tilde{a}$ и $\tilde{b}$ называются соседними, если расстояние Хемминга $\rho(\tilde{a},\tilde{b}) = 1$. Пару соседних вершин назовём ребром куба. Последовательность вершин куба $\tilde{a}_1,\tilde{a}_2,...,\tilde{a}_k$ называется цепью [3], если $\rho(\tilde{a}_i,\tilde{a}_{i+1}) = 1$, $i = \overline{1,k-1}$. Говорят, что вершина $\tilde{a}$ предшествует вершине $\tilde{b}$ $(\tilde{a} \le \tilde{b})$, если для их компонент выполнено $a_i \le b_i$, $i = \overline{1,n}$. Если $\tilde{a}$ не предшествует $\tilde{b}$ и $\tilde{b}$ не предшествует $\tilde{a}$, то вершины $\tilde{a}$ и $\tilde{b}$ несравнимы. Любое множество несравнимых вершин булева куба [3] называется антицепью. Антицепь называется максимальной, если любая вершина булева куба сравнима с одной из вершин этой антицепи. Слоем булева куба назовём множество входных наборов с одинаковым количеством единиц. Примеры булевых кубов представлены на рис. 1.

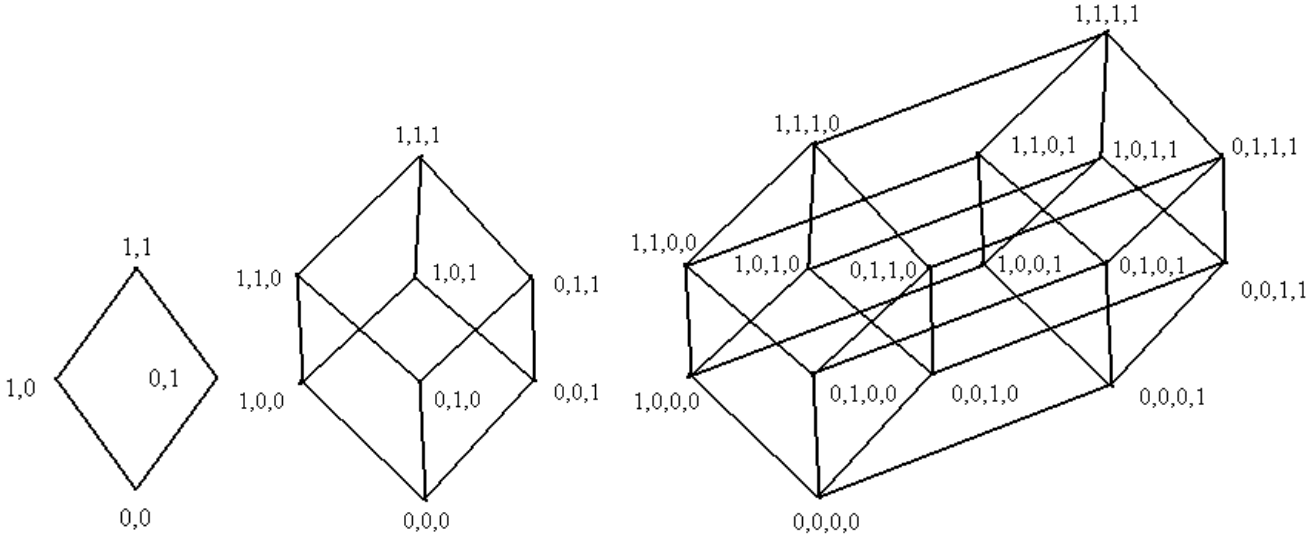


Рисунок 1 – Булевы кубы размерности 2, 3, 4

В булевом кубе ранга *n* можно выделить *n* пар непересекающихся кубов ранга *n* – 1. Для этого достаточно выбрать любую компоненту входного набора и определить нижний куб всеми входными наборами, где эта компонента равна 0, а верхний куб наборами, где она равна 1.

Рассмотрим один из способов описания МБФ [7] в виде минимальных входных наборов или соответствующего семейства подмножеств Шпернера. (Любое семейство подмножеств некоторого множества называется семейством подмножеств Шпернера, если ни одно из подмножеств семейства не содержится ни в каком другом подмножестве этого же семейства.) При этом если берется МБФ от *n* переменных, то произвольное подмножество семейства подмножеств Шпернера может содержать от 0 до *n* элементов. Семейство подмножеств Шпернера соответствует некоторой антицепи на булевом кубе.

Назовем вектор $T = (a_0, a_1,\ldots,a_i,\ldots,a_n)$ из $n + 1$ компоненты, которые нумеруются слева направо от 0 до *n*, типом МБФ, если *i*-я компонента вектора a_i равна числу подмножеств из *i* элементов в соответствующем данной МБФ семействе подмножеств Шпернера. При этом одновременно *i*-я компонента вектора a_i равна числу минимальных входных наборов данной МБФ, лежащих на слое $n - i$ булевого куба ранга *n*.

Назовем число n рангом типа T, число v ненулевых компонент назовем весом типа T, номер i первой слева ненулевой компоненты назовем левой границей типа T, номер j первой справа ненулевой компоненты правой границей типа T, сумму m всех компонент типа T назовём мощностью типа. Тип T называется максимальным, если при увеличении любой его компоненты на 1, полученный вектор не будет являться типом.

Пример 1. В качестве примера возьмем МБФ f от 5 переменных, равную единице на входных наборах 00011, 00111, 01011, 10011, 01111, 10111, 11011, 11100, 11101, 11110 и 11111. Минимальными входными наборами функции f являются наборы 00011 и 11100, первый из которых находится на уровне 3, а второй на уровне 2 булевого куба. В символьном виде МБФ имеет вид $f = x_2x_1 \vee x_5x_4x_3$. Отсюда соответствующее семейство подмножеств Шпернера состоит из двух подмножеств, первое из которых содержит два элемента, а второе три элемента. Значит тип Т(f) функции f равен (0, 0, 1, 1, 0, 0). Ранг этого типа n(Т) = 5, вес v(Т) = 2, левая граница i(Т) = 2, правая граница j(Т) = 3. Такой же тип имеет и еще ряд МБФ, в частности МБФ с минимальными входными наборами 00101 и 11001.

Назовём типы видов $(0,0,...,0),(1,0,...,0),(0,0,...,0,1)$ нулевым, левой и правой единицей соответственно. Для нулевого типа правая и левая единицы совпадают. Назовём типы нулевого ранга (0) и (1) базовыми нулём и единицей соответственно.

Расширим понятия ранга, веса, левой границы, правой границы и мощности для любого вектора, у которого все компоненты неотрицательные целые числа. Для любых двух векторов V_1, V_2 ранга n и таких, у которых правая граница $j(V_1)$ строго меньше левой границы $i(V_2)$, определим операцию сдвиг-суммы:

$$V = V_1 \circ V_2 = (a_0, a_1, ..., a_n) \circ (b_0, b_1, ..., b_n) = (b_0, a_0 + b_1, ..., a_{n-1} + b_n, a_n) = (c_0, c_1, ..., c_{n+1}).$$

Такую операцию с нулевым вектором $V_0 = (0,0,...,0)$ можно проводить как справа, так и слева:

$$V = V_1 \circ V_0 = (a_0, a_1, ..., a_n) \circ (0,0,...,0) = (0, a_0, ..., a_{n-1}, a_n)$$
$$V = V_0 \circ V_1 = (0,0,...,0) \circ (a_0, a_1, ..., a_n) = (a_0, ..., a_{n-1}, a_n, 0)$$

ЛЕММА 1. Операция сдвиг-суммы над любыми двумя допустимыми типами ранга n даёт тип ранга $n + 1$.

Доказательство. Пусть $T = T_1 \circ T_2 = (a_0, a_1, ..., a_n) \circ (b_0, b_1, ..., b_n) = (c_0, c_1, ..., c_{n+1})$. Произвольным образом разобьем булев куб ранга $n + 1$ на два куба ранга n. В верхнем кубе выберем МБФ f_1 типа T_1, а в нижнем f_2 типа T_2. Это всегда можно сделать по определению типа. По определению допустимой пары из неравенства $j(T_1) < i(T_2)$ следует, что ни один минимальный набор функции f_1 не больше ни одного минимального набора f_2. Следовательно, объединение минимальных входных наборов функций f_1 и f_2 образует антицепь на булевом кубе ранга $n + 1$. Минимальные наборы этой антицепи задают функцию f, которая по определению сдвиг-суммы имеет тип T. Лемма доказана.

Доказательство утверждения обратного лемме 1 (теорема 2 из [8] является таким утверждением для максимальных типов) путем разбиения произвольной МБФ в булевом кубе на две МБФ в верхнем и нижнем кубах невозможно. В качестве примера приведём МБФ 6-го ранга.

Пример 2. Рассмотрим МБФ

$$f = x_1x_2 \vee x_3x_4 \vee x_5x_6 \vee x_1x_3x_5 \vee x_1x_3x_6 \vee x_1x_4x_5 \vee x_1x_4x_6 \vee x_2x_3x_5 \vee x_2x_3x_6 \vee x_2x_4x_5 \vee x_2x_4x_6.$$

Эта функция имеет тип $(0,0,3,8,0,0,0)$, который не является максимальным, так как существует тип $(0,0,3,11,0,0,0)$. Ей соответствуют вершины с входными наборами 000011, 001100 и 110000 на 4-м уровне булева куба и вершины с входными наборами 010101, 100101, 011001, 101001, 010110,100110, 011010 и 101010 на 3-м уровне. Никакое разделение булева куба 6-го ранга на 2 куба 5-го ранга не приведёт к тому, что в один куб 5-го ранга войдут все 3 вершины с 4-го уровня либо 8 вершин с 3-го уровня. Следовательно, типы 2 МБФ, входящих в кубы 5-го ранга не составят допустимую пару типов. Антицепь, соответствующая этой функции, является максимальной, т.е. к ней нельзя добавить ни одной вершины куба.

В [8] показано, что для максимальных типов это разложение единственно. Для немаксимальных типов такое разложение может быть не единственным. Для однозначного разложения произвольного вектора введём операции выбора максимальной левой части и максимальной правой части. Сначала определим правую V_2 и левую часть V_1 для вектора V с номерами компонент от 0 до n, у которого компоненты 0 и n равны нулю.

Правой частью V_2 вектора V, у которого компонента n равна нулю, называется вектор с компонентами с нулевой по $n - 1$, у которого компоненты с $i + 1$ по $n - 1$ вектора V_2 совпадают с соответствующими компонентами вектора V, а i компонента вектора V_2 больше нуля и меньше или равна i-й компоненты вектора V (при этом i будет левой границей вектора V_2).

Левой частью V_1 вектора V, у которого компонента 0 равна нулю, называется вектор с компонентами с нулевой по $n - 1$, у которого компоненты с нулевой по $j - 1$ вектора V_1 совпадают с компонентами с первой по j вектора V, а j компонента вектора V_1 больше нуля и меньше или равна $j + 1$ компоненты вектора V (при этом j будет правой границей вектора V_1).

Если вектор n ранга является правой единицей, то его единственной правой частью является нулевой вектор n-го ранга, а левой частью правая единица n-го ранга. Если вектор n ранга является левой единицей, то его единственной левой частью является нулевой вектор n-го ранга, а правой частью левая единица n-го ранга. Если вектор n ранга является нулевым, то его левая и правая части совпадают и являются нулевым вектором n-го ранга. У базовых нуля и единицы ни левая, ни правая части не выделяются.

Таким образом, правая (левая) часть определены только для векторов, у которых компонента n (компонента 0) равна нулю (кроме базовых 0 и 1). Дополнительно для правой (левой) единицы (кроме базовой 1) определена правая (левая) часть, равная нулевому типу. Для вектора мощности m, у которого определена правая (левая) часть, имеется $m + 1$ различных правых (левых) частей мощности от 0 до m (по одной правой (левой) части для каждой мощности).

Остатком вектора V ранга $n + 1$ после выделения правой части V_2 называется вектор $n + 1$ ранга, получающийся вычитанием компонент с нулевой по $n - 1$ вектора V_2 из соответствующих компонент вектора V. Если нулевая компонента остатка равна нулю, то, отбрасывая эту нулевую компоненту из остатка, получаем вектор n-го ранга D_1, который назовём дополнением правой части V_2. Дополнение D_1 является левой частью вектора V и $D_1 \circ V_2 = V$. Остатком вектора V ранга $n + 1$, после выделения левой части V_1, называется вектор $n + 1$ ранга, получающийся вычитанием компонент с нулевой по $n - 1$ вектора V_1 из компонент с 1 по n-ю вектора V. Если n-я компонента остатка равна нулю, то, отбрасывая эту n-ю компоненту из остатка, получаем вектор n-го ранга D_2, который назовём дополнением левой части V_1. Дополнение D_2 является правой частью вектора V и $V_1 \circ D_2 = V$. Если нулевая (последняя) компонента остатка вектора V после выделения правой (левой) части не равна нулю и вектор V не равен правой (левой) единице, то правая (левая) часть вектора V не имеет дополнения и вектор V нельзя получить из двух векторов n-го ранга с помощью операции сдвиг-суммы.

Максимальной правой (левой) частью вектора $n + 1$ ранга называется его правая (левая) часть, являющаяся типом ранга n наибольшей возможной мощности. Из определения максимальной правой (левой) части для любого вектора следует, что она либо не определена (если не определена правая (левая) часть), либо единственна. Если для вектора $n + 1$ ранга нулевая и n-я компонента равна нулю, то из него по определению можно выделить как максимальную левую, так и максимальную правую части. Сокращённо будем называть разложение вектора, получающееся после выделения из него максимальной правой (левой) части правым (левым) разложением. Если вектор не является нулевым типом, правой или левой единицей, то мощность его максимальной правой (левой) части больше нуля.

Пример 3. Возьмём тип ранга 6: $T = (0,0,3,4,1,0,0)$, для него мы имеем такие разложения:

$$(0,0,3,4,1,0,0) = (0,3,0,0,0,0) \circ (0,0,0,4,1,0),$$

$$(0,0,3,4,1,0,0) = (0,3,1,0,0,0) \circ (0,0,0,3,1,0).$$

Первое разложение получается после выделения максимальной правой части, а второе - максимальной левой части. По определению правой (левой) части такие разложения будут единственными. Здесь $(0,3,0,0,0,0)$ является дополнением максимальной правой части, а $(0,0,0,3,1,0)$ – дополнением максимальной левой части. В примере 2 тип $(0,0,3,8,0,0,0)$ имеет единственное правое разложение $(0,3,0,0,0,0) \circ (0,0,0,8,0,0)$ и единственное левое разложение $(0,3,1,0,0,0) \circ (0,0,0,7,0,0)$.

2. Деревья типов МБФ. Так как для кодирования информации в виде блоков переменной длины предлагается использовать деревья типов, то нужно доказать, что любому типу однозначно соответствует некоторое бинарное дерево. Вначале, на основе ранее введенных понятий, докажем теорему об однозначном разложении типов, которая обратна лемме 1.

ТЕОРЕМА 1. Любой тип ранга $n+1$ имеет однозначное правое (левое) разложение на два типа ранга n.

Доказательство. Пусть из типа T ранга $n+1$ выделена максимальная правая часть T_2. По определению максимальной правой части такое выделение выполняется однозначно из любого типа ранга больше 0 и при этом T_2 является типом ранга n. Для любого типа T определено также дополнение D_1 максимальной правой части T_2, причем $T = D_1 \circ T_2$. Остается доказать, что D_1 является типом. Построим в булевом кубе ранга $n+1$ антицепь из минимальных входных наборов МБФ типа T. Выражение $T = D_1 \circ T_2$, где T и T_2 типы, означает, что в булевом кубе ранга $n+1$ существует антицепь A, причем часть вершин антицепи A образуют антицепь A_2 из минимальных входных наборов МБФ типа T_2. Это означает, что антицепь A_2 лежит в некотором нижнем подкубе ранга n булева куба ранга $n+1$. Докажем, что остальные вершины антицепи A, которые образуют антицепь A_1, лежат в соответствующем верхнем подкубе ранга n. Заметим, что по определению допустимой пары, должно выполнятся условие $j(D_1) < i(T_2)$, а это означает, вершины антицепи A_1 находятся не выше вершин антицепи A_2. Далее, если бы хотя бы одна вершина из A_1 лежала в нижнем подкубе, то из типа T можно было бы выделить максимальную правую часть большей мощности, чем мощность типа T_2. Это невозможно, так как по определению максимальная правая часть выделяется однозначно. Следовательно, антицепь A_1 лежит в верхнем подкубе и вершины этой антицепи соответствуют минимальным входным наборам некоторой МБФ с типом D_1 ранга n. Значит тип T имеет правое разложение $D_1 \circ T_2$. Аналогично доказывается, что тип T имеет левое разложение $T_1 \circ D_2$. Теорема доказана.

Следствие 1. Если из типа ранга $n+1$ выделить максимальную правая (левую) часть ранга n, то дополнение также будет типом ранга n.

Следствие 2. Если из вектора ранга $n+1$ (не типа) выделить максимальную правую (левую) часть ранга n, то дополнение либо не определено, либо будет вектором ранга n (не типом).

Из этой теоремы также следует второе (более простое) доказательство теоремы 2 из [8].

ТЕОРЕМА 2. Любой максимальный тип ранга $n+1$ имеет однозначное разложение на два максимальных типа ранга n.

Доказательство. Согласно теореме 1 любой максимальный тип ранга $n+1$ имеет однозначное правое разложение $T = T_1 \circ T_2$, где T_1 и T_2 типы ранга n. Пусть T_1 не является максимальным типом. Тогда существует максимальный тип $T_3 > T_1$ и по лемме 1 $T_5 = T_1 \circ T_3$, где T_5 тип ранга $n+1$ и $T_5 > T$. Так как T максимальный тип , то это невозможно. Следовательно T_1 – максимальный тип. Аналогично T_2 также максимальный тип. Совпадение правого и левого разложения следует из леммы 1 из [8]. Теорема доказана.

Так как не каждый вектор является типом МБФ, то необходим удобный критерий для определения, является ли вектор типом. Один такой критерий [6] основан на построении модельной МБФ. Рассмотрим другой критерий.

ЛЕММА 2. Вектор $V = (a_0, a_1, ..., a_n)$ не является типом МБФ, если в процессе последовательного выделения максимальной правой (левой) части на каком-то этапе получаем остаток, для которого не определено дополнение максимальной правой (левой) части соответственно.

Доказательство. Если максимальная правая (левая) часть не определена для исходного вектора V, то теорема доказана. В противном случае рассматриваем правое (левое) разложение $D_1 \circ V_2 = V$ ($V_1 \circ D_2 = V$) из теоремы 1. Согласно следствию 2 теоремы 1 $D_1(D_2)$ не является типом. Продолжаем выделение максимальной правой (левой) части из $D_1(D_2)$, пока после выделения правой (левой) части для остатка определено дополнение, т.е. нулевая компонента не станет больше нуля. При этом мощность максимальной правой (левой) части $V_2(V_1)$ больше нуля. Следовательно, мощность дополнения $D_1(D_2)$ будет на каждом шаге уменьшаться, кроме того, левая граница дополнения будет сдвигаться на единицу влево и на каком-то этапе станет равной нулю. Мощность дополнения не может быть равна 0 или 1, так как все вектора с мощностями 0 и 1 являются типами. Поэтому, когда левая граница станет равной нулю, мощность дополнения будет больше единицы. Это возможно в двух случаях, когда больше 1 нулевая компонента либо когда нулевая компонента равна 1, а в дополнении есть другие ненулевые компоненты. Очевидно, что в обоих случаях $D_1(D_2)$ не является типом. Лемма доказана.

Пример 4. Рассмотрим вектор 6 ранга $(0,0,4,1,4,0,0)$. Его правое разложение равно $(0,4,1,0,0,0) \circ (0,0,0,0,4,0)$. Правое разложение вектора $(0,4,1,0,0,0) = (2,0,0,0,0) \circ (0,2,1,0,0)$. Вектор $(2,0,0,0,0)$ правого разложения в виде сдвиг-суммы, по определению, не имеет. Следовательно, вектор $(0,0,4,1,4,0,0)$ не является типом. Этот вектор является единственным вектором 6 ранга, который не является типом и который не сравним ни с одним типом 6-го ранга.

Разложение любого типа можно представить в виде двоичного дерева. Концевыми вершинами этого дерева могут быть базовые типы (0) и (1), назовём такое дерево разложения полным. Полное дерево имеет $2^{n+1} - 1$ вершин. Назовём дерево правым (левым), если мы получаем его в результате выделении правой (левой) части и если его концевыми вершинами является правые единицы, левые единицы и нулевые типы различных рангов. Для максимальных типов левое и правое деревья совпадают.

ЛЕММА 3. Любой тип можно разложить до полного, правого и левого дерева. Концевыми вершинами полного дерева являются базовые ноль и единица нулевого ранга. Концевыми вершинами правого (левого) дерева являются нулевой тип, левая или правая единицы различных рангов. Для максимальных типов левое и правое деревья совпадают, а концевыми вершинами этого дерева являются только левая и правая единицы различных рангов.

Доказательство. Пусть тип является нулевым типом *n*-го ранга. По определению он разлагается на два нулевых типа $n-1$ ранга. Продолжая этот процесс для каждого из двух типов разложения, получаем полное дерево, так как в результате придем к нулевым типам нулевого ранга. Пусть тип является правой (левой) единицей *n*-го ранга. По определению он разлагается на два типа: нулевой и правую единицу $n-1$ ранга (левую единицу и нулевой $n-1$ ранга). Этот процесс можно повторять пока не получим типы нулевого ранга, т.е. опять получается полное дерево.

Докажем теперь возможность разложения до нулевого типа, правой (левой) единицы. Пусть тип *n*-го ранга не равен нулевому, левой и правой единицы. Тогда возможно единственное правое разложение этого типа на два допустимых типа $n-1$ ранга, второй из которых является максимальной правой частью, а первый дополнением этой части. После каждого выделения максимальной правой части отбрасывается правая крайняя компонента и в результате на некотором

этапе получается, что ненулевая компонента становится крайней справа. Если эта компонента больше единицы, то по лемме 2 исходный вектор не является типом. Значит, полученный вектор равен правой единице. Максимальная правая часть такого разложения никогда не равна нулевому вектору. Значит, мощность левой части на каждом этапе уменьшается пока не доходит до нуля либо до единицы. Если мощность вектора равна единице и он не является левой единицей, то из него можно выделить максимальную правую часть с мощностью единица, левое дополнение которой будет нулевым вектором. Таким образом, доказано, что с помощью операции выделения максимальной правой части можно построить дерево разложения типа МБФ до нулевого типа, левой или правой единицы, т.е. получить разложение в виде правого дерева. Аналогично доказывается, что можно получить левое дерево. По доказанному выше можно продолжить разложение правой (левой) единицы и нулевого типа ненулевого ранга до базовых нулей и единиц нулевого ранга. В результате получаем полное дерево. Если исходный тип является максимальным (кроме правой или левой единицы), то по теореме 2 он разлагается на два максимальных типа. Правое и левое дерево при этом совпадают. Так как нулевой вектор не является максимальным типом, то при разложении максимального типа ни левая, ни правая часть не может быть нулевым типом. Следовательно, правое (левое) дерево разложения максимального типа в качестве концевых вершин может иметь только правую или левую единицу. Лемма доказана.

Пример 5. Рассмотрим пример построения дерева (рис. 2) для типа 6-го ранга $(0,0,3,4,1,0,0)$, будем выбирать разложения с максимальной правой частью:

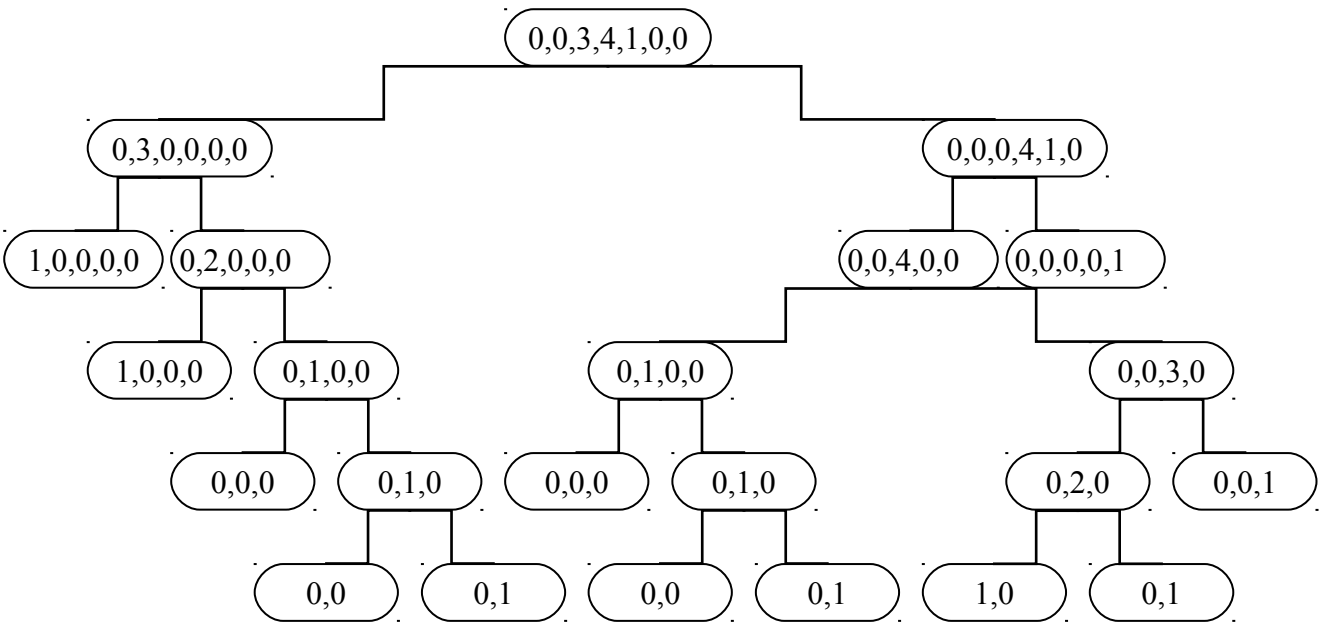


Рисунок 2 – Правое дерево разложения 6-го ранга типа $(0,0,3,4,1,0,0)$

Это разложение можно записать в виде формулы следующим образом:

$$(0,0,3,4,1,0,0) = (0,3,0,0,0,0)\circ(0,0,0,4,1,0) =$$
$$= ((1,0,0,0,0)\circ(0,2,0,0,0))\circ((0,0,4,0,0)\circ(0,0,0,0,1)) =$$
$$= ((1,0,0,0,0)\circ((1,0,0,0)\circ(0,1,0,0)))\circ(((0,1,0,0)\circ(0,0,3,0))\circ(0,0,0,0,1)) =$$
$$= [(1,0,0,0,0)\circ((1,0,0,0)\circ((0,0,0)\circ((0,0)\circ(0,1))))]\circ$$
$$\circ[(((0,0,0)\circ((0,0)\circ(0,1)))\circ(((0,0)\circ(0,1))\circ(0,0,1)))\circ(0,0,0,0,1)] \quad .$$

Пример 6. Рассмотрим примеры деревьев разложения максимальных типов ранга 4 (рис. 3).

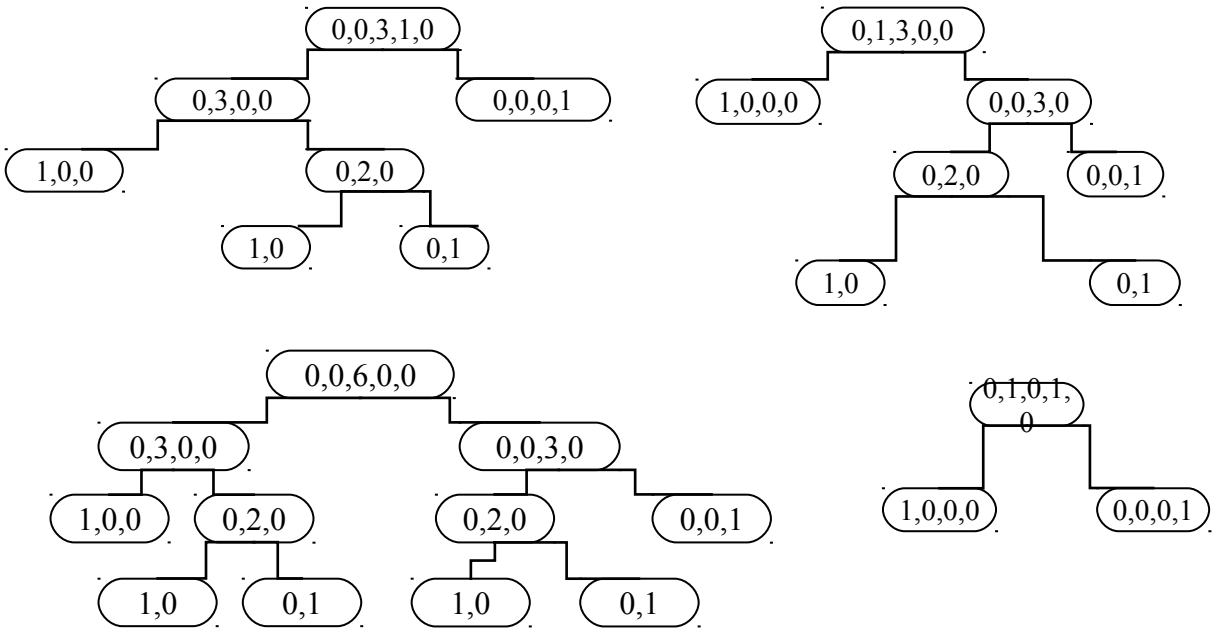


Рисунок 3 – Деревья разложения максимальных типов ранга 4

Пример 7. Рассмотрим полное дерево разложения 4 ранга (рис. 4).

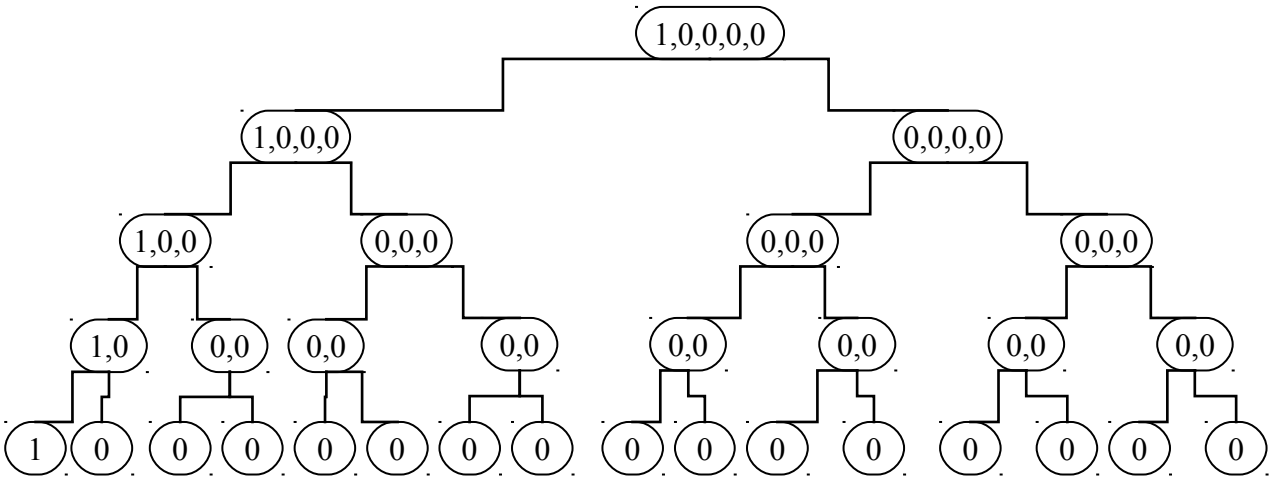


Рисунок 4 – Полное дерево разложение

3. Построение шифротекста. Построение будем проводить по следующей схеме (рис. 5):

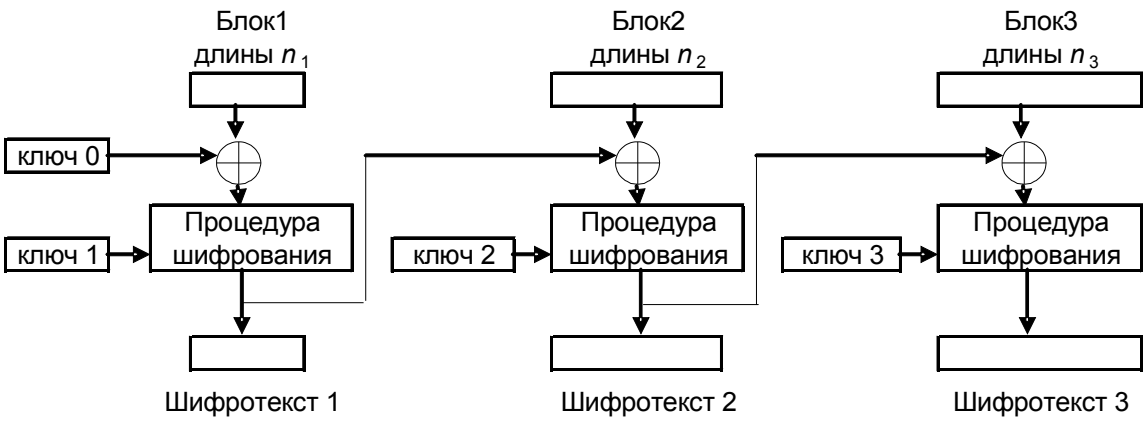


Рисунок 5 – Схема шифрования с блоками переменной длины

Весь открытый текст разбиваем на блоки. Блоки сцепляем следующим способом: результат шифрации предыдущих блоков суммируется по модулю 2 (исключающее «ИЛИ», XOR) с открытым текстом следующего блока. Для первого блока используем нулевой ключ. Таким образом, любой блок шифра зависит не только от исходного текста, но и от всех предыдущих блоков текста. Блоки могут быть фиксированной длины либо переменной.

В качестве ключей шифрования (для каждого блока различный) используем цифры, стоящие в вершинах деревьев, неравных 0. Вершины деревьев будем обходить каким-либо способом, например, сверху вниз и слева направо. В результате получим последовательность чисел – ключ. Так для дерева из примера 5 последовательность чисел будет выглядеть таким образом: 3,4,1,1,2,4,1,1,1,1,1,3,1,1,1,1,1,1,1,1.

Такой ключ довольно простой, так как ранг дерева равен 6 и количество вершин $\le 2^7 - 1$. Учитывая, что с увеличением ранга количество типов сильно возрастает:

Ранг	1	2	3	4	5	6	7	8	9	10
Кол. типов	3	5	10	26	96	553	5461	100709	3718354	289725509

Если взять тип более высокого ранга, то получим ключ, которым можно шифровать довольно большие блоки текста.

Процедура шифрования заключается в перестановки битов сообщения с помощью ключа. Например, для ключа, приведенного выше.

Номер бита сообщения	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Перестанавливаем с битом под номером	3	4	1	1	2	4	1	1	1	1	1	3	1	1	1	1	1	1	1	1

Получаем такую перестановку: первый бит сообщения меняем с 3-м битом , затем 2-й бит переставляем с 4-м и т.д. В ключе берём столько чисел, сколько битов в блоке. Так как количество вершин в дереве ранга n превосходит $2n$, то ранг ключа должен быть больше половины длины блока. Если какое-либо число в ключе больше длины блока, то вместо него записываем остаток от деления этого числа на длину блока.

Дешифрование будем проводить в обратном порядке и по такой схеме (рис. 6):

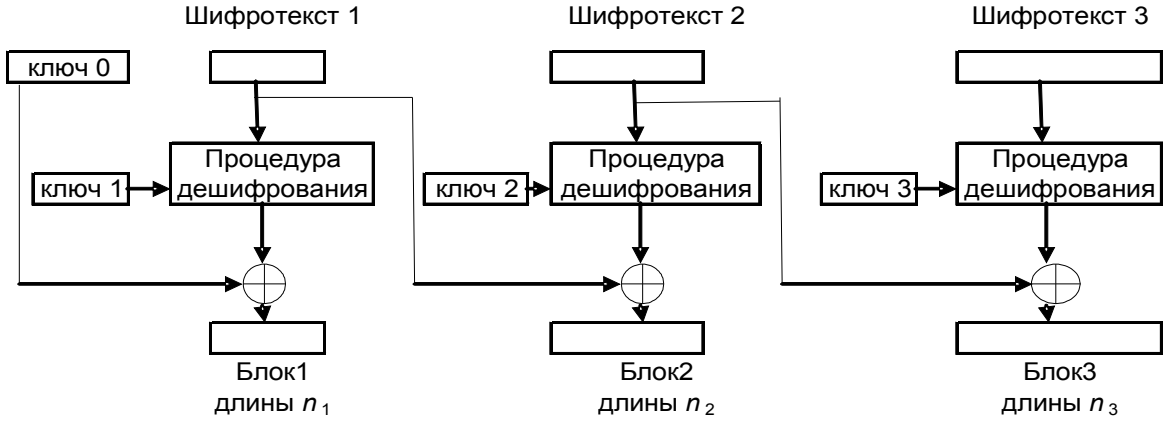
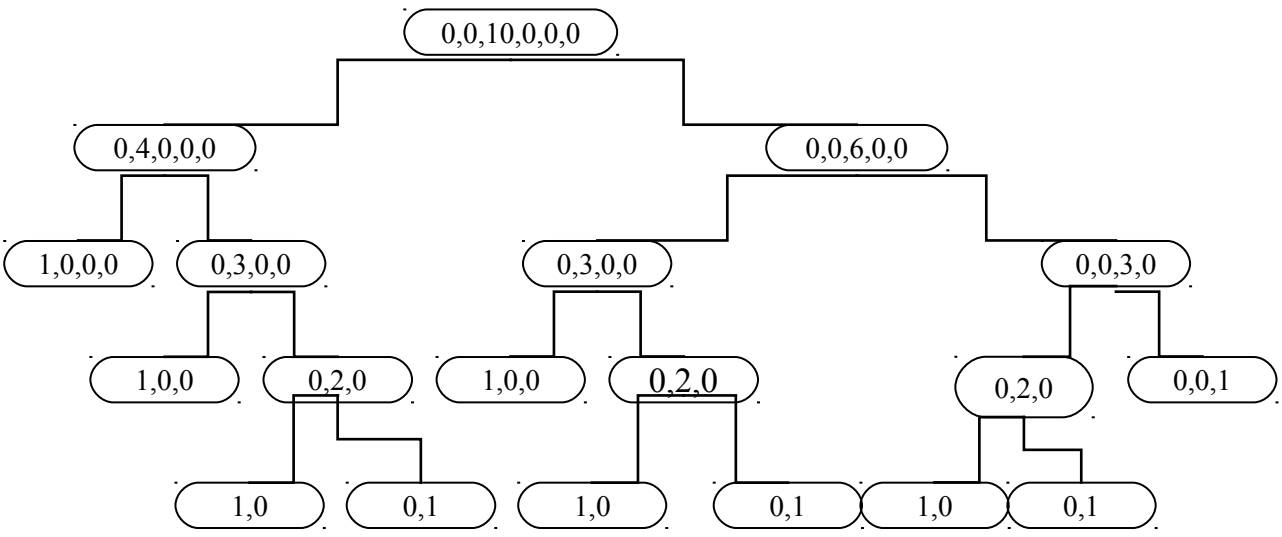


Рисунок 6 – Схема дешифрования с блоками переменной длины

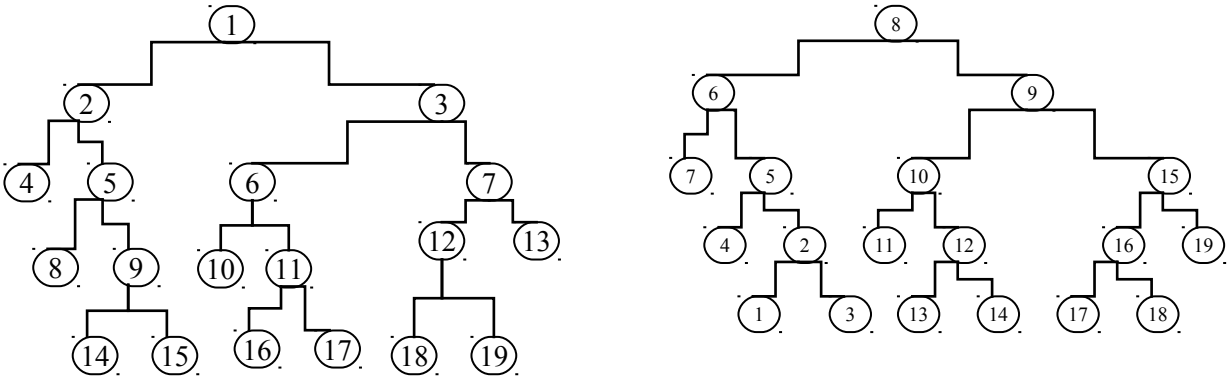
В секретную часть информации для такой схемы шифрования будут входить деревья соответствующего ранга, служащие в качестве ключей к блокам и записанные последовательностью чисел, длины блоков, если блоки переменной длины. В этом случае ключ выбирается по длине блока, а для операции исключающего «ИЛИ» недостающую часть заполняем нулями. Эту часть информации можно передавать по защищенному каналу, например, используя криптографию с открытым ключом.

Построение ключей можно проводить по другой схеме. Перестановку битов осуществлять разными обходами вершин деревьев типов. Например, пронумеруем вершины дерева, начиная сверху к низу и слева направо. Это будут номера битов сообщения, назовём это прямым обходом. Далее, получим номера битов, с которыми будем осуществлять перестановку. Обход вершин дерева сделаем следующим образом: начинаем слева снизу вершина № 1, затем фиксируем вершину, которая на уровень выше, вершина № 2, и обходим все нижние вершины и т.д., назовём это обратным обходом. Всё сказанное рассмотрим на примере.

Пример 8. Получим дерево разложения максимального типа 5-го ранга $(0, 0, 10, 0, 0, 0)$ и построим для него прямой и обратный обходы (рис. 7).



а)



б) в)

Рисунок. 7 – а) дерево разложения типа 5-го ранга (0,0,10,0,0,0), б) прямой обход, в) обратный обход

В этом случае таблица перестановки битов будет выглядеть так:

Номер бита сообщения	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Перестанавливаем с битом под номером	8	6	9	7	4	10	15	5	2	11	12	16	19	1	3	13	14	17	18

В заключение отметим следующее. Для получения максимальных типов, всех типов *n*-го ранга, а также реализации описанных алгоритмов шифрации и дешифрации была разработана экспериментальная программа в среде программирования Delphi. Так как максимальные типы одного ранга имеют между собой кодовое расстояние (расстояние Хэмминга), увеличивающиеся с ростом ранга, то эти типы МБФ можно использовать как корректирующий код. Это предполагается рассмотреть в следующей статье. В дальнейшей работе планируется дать оценку криптографической стойкости полученного криптоалгоритма по отношению к известным криптографическим атакам. Для типов достаточно больших рангов при определённом выборе обхода дерева типа МБФ цифры ключа не будут зависеть друг от друга. Также используя типы больших рангов, возможно, создать криптосистему с открытым ключом, если найти процедуру шифрования, не использующую разложение этих типов и процедуру дешифрования, использующую это разложение. В настоящее время эффективная процедура разложения больших типов неизвестна. В то же время типы большого ранга легко можно получить с помощью операции сдвиг-суммы типов малых рангов.

Литература

1. *Гатчин Ю.А.* Основы криптографических алгоритмов: учебное пособ. / Ю.А. Гатчин, А.Г. Коробейников. – С.Пб: С.Пб ГИТМО (ТУ), 2002. – 29 с.
2. *Чмора А.Л.* Современная прикладная криптография. – [2-е изд.] / Чмора А.Л. – М.: Гелиос АРВ, 2002. – 256 с.
3. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М.А. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
4. *Коробейников А.Г.* Математические основы криптографии: учеб. пособ. / Коробейников А.Г. – С.Пб: С.Пб ГИТМО (ТУ), 2002. – 41 с.
5. *Аграновский А.В.* Классические шифры и методы их криптоанализа / А.В. Аграновский, А.В Балакин, Р.А. Хади // Машиностроение: Информационные технологии. – 2001. – № 10 – С. 40 – 45.
6. *Ткаченко В.Г.* Классификация монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 2008. – № 1. – С. 35 – 43.
7. *Ткаченко В.Г.* Отказы цифровых схем и представления монотонных булевых функций / В.Г. Ткаченко //Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 2006. – № 2. – С. 45 – 69.
8. *Ткаченко В.Г.* Перечисления типов монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 2008. – № 2. – С. 54 – 69.