МЕТОДЫ ПОИСКА МАКСИМАЛЬНЫХ СОВМЕСТНЫХ ПОДСИСТЕМ СИСТЕМ БУЛЕВЫХ УРАВНЕНИЙ

Байжуманов А.А. *[1][0000-0002-4315-4734]*, ***Бердимуров М.А.*** *[2][0000-0002-3031-5009]*, ***Кудайбергенов А.А.*** *[3][0000-0002-2630-5182]*

[1]Южно-Казахстанский государственный университет, к.ф.-м.н., доцент, E-mail: absattar52@mail.ru

[2]Старший преподаватель кафедры “Современные информационные и коммуникационные технологии” Международной исламской академии Узбекистана, PhD., E-mail: m.berdimurodov@iiau.uz

[3]Докторант Национального университета Узбекистана им.Мирзо Улугбека, PhD, доцент, E-mail: q_adilbay@karsu.uz.

Annotatsiya. Ushbu maqolada, amaliy masalalarni yechishning evristik usullarining aniqligini oshirish maqsadida, mantiqiy tenglamalar tizimlarini yechish vazifasi taqdim etilgan. Bu vazifa algebraik kriptoanaliz, prognozlash, tanib olish, tasniflash va ko'plab o'zgaruvchilar to'plamining mutlaq ekstremumlarini qidirish sohalaridagi amaliy masalalar uchun qo'llaniladi. Shuningdek, dekodlash vazifasini yechish va monoton mantiqiy funksiyalarning maksimal yuqori nolini topish orqali mantiqiy tenglamalar tizimlarining maksimal kichik tizimlarini qidirish algoritmi ishlab chiqilgan.
Kalit so‘zlar: algoritm, evristik usul, butun sonli tenglamalar, mutlaq ekstremum, dekodlash, monoton mantiqiy funksiya, tizim.

Аннотация. В статье представлена задача поиска решений систем булевых уравнений с целью повышения точности эвристических методов решения практических задач алгебраического криптоанализа, прогнозирования, распознавания, классификации и поиска абсолютных экстремумов множества переменных. Также путем решения задачи декодирования и нахождения максимального верхнего нуля монотонных логических функций был разработан алгоритм поиска максимальных подсистем систем логических уравнений.
Ключевые слова: алгоритм, эвристический метод, булевых уравнений, абсолютный экстремум, декодирования, монотонная логическая функция, система.

Annotation. The article presents the problem of finding solutions to systems of Boolean equations in order to increase the accuracy of heuristic methods for solving practical problems of algebraic cryptanalysis, forecasting, recognition, classification and search for absolute extrema of many variables. Also, by solving the problem of decoding and finding the maximum upper zero of monotonic logical functions, an algorithm for searching for maximum subsystems of systems of logical equations was developed.
Key words: algorithm, heuristic method, Boolean equations, absolute extremum, decoding, monotonic logical function, system.

Введение

В настоящее время в мире особое внимание уделяется использованию информационных технологий в различных отраслях, в особенности в сфере применения их в государственном управлении и системе самоуправления, актуальной проблемой является применение технологий и методов обеспечения корректности информации в цифровой экономике, при предоставлении физическим и юридическим лицам различных государственных интерактивных услуг, расширения возможностей интеграции хозяйственных систем в мировом масштабе. Поэтому для обеспечения выполнения постановления особое значение приобретает проблема поиска решений систем булевых уравнений для повышения точности эвристических методов решения прикладных задач алгебраического

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

криптоанализа, прогнозирования, распознавания, классификации, поиска абсолютных экстремумов функций многих переменных [1-3].

1. Об одном алгоритме поиска максимального верхнего нуля монотонных булевых функций.

Пусть E_n^2 - n - мерный двочный куб. Нормой $|\tilde{\alpha}|$ набора $\tilde{\alpha}$ в E_n^2 назовем число единичных элементов. Число $A_{\tilde{\alpha}} = \sum_{i=1}^{n} \alpha_i \cdot 2^{n-i}$ будем называть номером $\tilde{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$. Будем говорит, что наборы $\tilde{\alpha}$ k-го уровня упорядочены в лексикографическом порядке, если они расположены в порядке убывания наборов $A_{\tilde{\alpha}}$ [4-5].

Считаем, что набор $\tilde{\beta}$ непосредственно следует за $\tilde{\alpha}$ на k -м уровне, $k = \overline{1, n}$, если $A_{\tilde{\beta}} < A_{\tilde{\alpha}}$ и не существует такого $\tilde{\gamma}$, где $|\tilde{\gamma}| = k$, что $A_{\tilde{\beta}} < A_{\tilde{\gamma}} < A_{\tilde{\alpha}}$.

Определение-1. Функция $f(x_1, x_2, ..., x_n)$ называется монотонной, если для любых двух наборов $\tilde{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$ и $\tilde{\beta} = (\beta_1, \beta_2, ..., \beta_n)$ таких, что $\alpha_1 \le \beta_1, \alpha_2 \le \beta_2, ..., \alpha_n \le \beta_n$ имеет место неравенство $f(\tilde{\alpha}) \le f(\tilde{\beta})$.

Пусть M_n – множество всех монотонных булевых функций от n переменных. Набор $\tilde{\alpha} \in E_n^2$ назовем верхним нулем функции $q \in M_n$, если $q(\tilde{\alpha}) = 0$ и для любого набора $\tilde{\beta} \in E_n^2$, $|\tilde{\alpha}| \le |\tilde{\beta}|$ следует, что $q(\tilde{\beta}) \ne 0$.

Верхний нуль $\tilde{\alpha}$ функции $q \in M_n$ называется ее максимальным верхним нулем (м.в.н.), если для верхнего нуля $\tilde{\beta}$ функции q будет $|\tilde{\beta}| \le |\tilde{\alpha}|$.

Пусть произвольная функция $q \in M_n$ задана при помощи оператора A_q, который по любому набору $\tilde{\alpha} \in E_n^2$ выдает значение $q(\tilde{\alpha})$. Задача поиска м.в.н. функций из M_n - формируется следующим образом. Если некоторая функция $q \in M_n$ задана оператором A_q, то требуется минимальным числом обращений к A_q найти хотя бы один м.в.н. функции $q(x_1, x_2, ..., x_n)$.

Опишем алгоритм A_M, где используется лексикографический порядок расположение наборов уравнений E_n^2.

Алгоритм A_M состоит из двух этапов:

Этап I. На первом шаге алгоритма вычесляем значение q на наборе $\tilde{\alpha}_1$ с наибольшим номером $\left[\frac{n}{2}\right]$–го уровня.

Пусть на i-м шаге вычеслено значение q на некотором наборе $\tilde{\alpha}_i$ $\left[\frac{n}{2}\right] - i + 1$-го уровня, $1 \le i \le \left[\frac{n}{2}\right]$. Если $q(\tilde{\alpha}_i) = 1$, то на $(i+1)$–м шаге вычисляем значение q на наборе $\tilde{\alpha}_{i+1}$ с наибольшем номером $\left[\frac{n}{2}\right] - i$–го уровня. Если же $q(\tilde{\alpha}_i) = 0$, то

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

переходим по второму этапу алгоритма. Если на $\left[\frac{n}{2}\right]+1$–м шаге получено $q\left(\alpha_{\left[\frac{n}{2}\right]+1}\right)=1$, то $q=1$ и алгоритм заканчивает работу.

Этап II. Пусть к началу второго этапа алгоритма сделано $\tau+1$ шагов $\left(0\le\tau\le\left[\frac{n}{2}\right]\right)$, т.е. вычеслены значения $q(\tilde{\alpha}_1)=q(\tilde{\alpha}_2)=...=q(\tilde{\alpha}_\tau)=1$ и $q(\tilde{\alpha}_{\tau+1})=0$, где $\tilde{\alpha}_1,\tilde{\alpha}_2,...,\tilde{\alpha}_{\tau+1}$ – с наибольшими номерами $\left[\frac{n}{2}\right],\left[\frac{n}{2}\right]-1,...,\left[\frac{n}{2}\right]-\tau$ – уровней соответственно. Тогда на $(\tau+2)$–м шаге вычисляем значение q на наборе $\tilde{\alpha}_{\tau+2}$ $\left[\frac{n}{2}\right]-\tau+1$–го уровня, непосредственно следующем за $\tilde{\alpha}_\tau$ в лексикографическом порядке, на котором значение q еще не определено. Причем, если $\tau=0$, то за $\tilde{\alpha}_{\tau+2}$ берем крайный левый набор уровня $\left[\frac{n}{2}\right]-i+1$.

Пусть на i-м шаге $(i\ge\tau+2)$ вычеслено значение q на некотором наборе $\tilde{\alpha}_i$ j-го уровня, где $j\ge\left[\frac{n}{2}\right]-\tau+1$. Если $q(\tilde{\alpha}_i)=1$, то на $(i+1)$–м шаге вычисляем значение q на наборе $\tilde{\alpha}_{i+1}$ того же j-го уровня, непосредственно следующем в лексикографическом порядке за $\tilde{\alpha}_i$. Если такого набора не существует, то алгоритм заканчивает работу. Если же $q(\tilde{\alpha}_i)=0$, то на $(i+1)-$м шаге вычисляем значение q на наборе $\tilde{\alpha}_{i+1}$ $(j+1)-$го уровня, непосредственно следующем в лексикографическом порядке за набором $\tilde{\alpha}$ с наименованием номеров $(j+1)-$го уровня таким, что $q(\tilde{\alpha})$ определена непосредственно или по монотонности и $q(\tilde{\alpha})=1$. Причем, если набор $\tilde{\alpha}$ не существует, то за $\tilde{\alpha}_{i+1}$ берем набор с наибольшим номером $(j+1)-$го уровня. В случае, когда не существует набор $\tilde{\alpha}_{i+1}$, удовлетворяющий указанным свойствам, алгоритм останавливается.

Пусть алгоритм сделал r шагов до остановки. Получаем цепочку наборов $\tilde{\alpha}_1,\tilde{\alpha}_2,...,\tilde{\alpha}_r$, на которых последовательно вычислялось значение q. Тогда м.в.н. функции q – это такой набор $\tilde{\alpha}_s$ на этой цепочки с максимальным s, что $q(\tilde{\alpha}_s)=0$. Действительно, из описания алгоритма следует, что на всех наборах $|\tilde{\alpha}_s|+1-$го уровня функции q определена по монотонности или непосредственно и равне единице [6-8].

2. Решение задачи поиска максимальных совместных подсистем.

Пусть дана система булевых уравнений:

$$M=\begin{cases} f_1(x_1,x_2,...,x_n)=1 \\ f_2(x_1,x_2,...,x_n)=1 \\ ..... \\ f_m(x_1,x_2,...,x_n)=1 \end{cases} \quad (1)$$

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

Определение-2. Весом P_i уравнения $f_i,\ i=\overline{1,m}$ назовем число всех $f_i \in M$ таких, что $f_i \cdot f_i \neq 0,\ i \neq j$.

Пусть $\alpha_{i_1},\alpha_{i_2},...,\alpha_{i_k}$ суть единичные координаты набора $\tilde{\alpha}=(\tilde{\alpha}_1,\tilde{\alpha}_2,...,\tilde{\alpha}_m) \in E_m^2$.

Рассмотрим монотонную булевую функцию $q(y_1,y_2,...,y_m)$:

$$q(y_1,y_2,...,y_m)=\begin{cases}0, & \text{если } \{f_{i_1}=1,\ f_{i_2}=1,...,\ f_{i_k}=1\} \text{ совместна},\\ 1- & \text{в противном случае.}\end{cases}$$

Для нахождения максимальной совместной подсистемы системы (1) применяем алгоритм A_M поиска максимального верхнего нуля (м.в.н.) функции $q(y_1,y_2,...,y_m)$. Причем поиск м.в.н. функции $q(\tilde{y})$ ведется в лексикографическом порядке наборов переменных $y_{i_1},y_{i_2},...,y_{i_m}$, для которых $P_{i_1} \geq P_{i_2} \geq ... \geq P_{i_m}$. На каждом шаге обращение к оператору O_q для вычисления значений $q(\alpha_1,\alpha_2,...,\alpha_m)$ на наборе $\tilde{\alpha}=(\alpha_1,\alpha_2,...,\alpha_m)$ у которого $\alpha_{i_1},...,\alpha_{i_k}$ суть единичные координаты, используем процедуру распознавания совместности подсистемы $\{f_{i_1}=1,\ f_{i_2}=1,...,\ f_{i_k}=1\}$ системы (1).

Исследуем процесс вычисления значений $q(y_1,y_2,...,y_m)$ на наборе E_n^2.

Пусть

$$\begin{cases} f_{l_1}(x_1,x_2,...,x_n)=1\\ f_{l_2}(x_1,x_2,...,x_n)=1\\ \quad\quad ..... \\ f_{l_t}(x_1,x_2,...,x_n)=1 \end{cases} \tag{2}$$

подсистема системы (1). Рассмотрим матрицу $\|a_{ij}\|_{t\times t}$:

$$a_{ij}=\begin{cases}1, & \text{если } f_{l_i}\cdot f_{l_{ij}} \neq 0,\ i,j=\overline{1,t};\\ 0- & \text{в противном случае.}\end{cases}$$

Очевидно, что матрица $\|a_{ij}\|_{t\times t}$ симметрична и, если система (2) совместна, то $f_{l_i}\cdot f_{l_{ij}} \neq 0,\ i,j=\overline{1,t}$, и соответственно, в этом случае $\|a_{ij}\|_{t\times t}$-однородно-единичная матрица. В дальнейшем мы будем так называть те матрицы, все элементы которой равны единице. Если в матрице $\|a_{ij}\|_{t\times t}$ имеется хотя бы один элемент $a_{ij}=0$, система несовместна.

Положим, что высказывания $f_i,\ i=\overline{1,m}$ системы (1) заданы в базисе:

$\{\bar{x},\ x_1\wedge x_2,\ x_1\vee x_2\}$.

Пусть подсистема (2) имеет вид:

$$\begin{cases} U_{11}\vee U_{12}\ \vee ...\vee U_{1p_1}=1\\ U_{21}\vee U_{22}\vee ...\vee U_{2p_2}=1\\ \quad\quad ..... \\ U_{t1}\vee U_{t2}\ \vee ...\vee\ U_{tp_t}=1 \end{cases} \tag{3}$$

Определим условия совместности системы (3). Нетрудно заметить, что система (3) совместна в том и только в том случае, если существует э.к. $U_{1j_1},U_{2j_1},...,U_{tj_1}$, такие что

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

$$\bigwedge_{k=1}^{t} U_{kj_k} \neq 0. \quad (4)$$

Предлагаем одну из эффективных процедур проверки (ПП) выполнения условия (4). Представим д.н.ф. $N_i, i=\overline{1,t}$ системы (3) в ортогональной д.н.ф. $N_i^0 = K_{i1} \vee K_{i2} \vee ... \vee K_{it_i}$. Индукцией по i, $(i=\overline{1,t-1})$ определяем совместность системы.

1-шаг индукции. Для э.к. K_{1j}, $j=\overline{1,t_1}$ д.н.ф. N_i^0 фиксируем э.к. $K_{21}, K_{22}, ..., K_{2k}$ в д.н.ф. N_2^0 такие, что $K_{2i} \cdot K_{1j} \neq 0$, $i=\overline{1,k}$.

Пусть $\tilde{T}_j = \{\Im_1, \Im_2, ..., \Im_k\}$, где $\Im_i = K_{2i} \cdot K_{1j} \neq 0$, $i=\overline{1,k}$. Причем, если очередного K_{2i} имеет место $K_{1j} \to K_{2i} = 1$, то $\tilde{T}_j = \{\Im_1\}$, где $\Im_1 = K_{1j} \cdot K_{2i} = K_{1j}$.

Положим $T_1 = \bigvee_{j=1}^{t_1} \tilde{T}_j$. В случае, когда $T_1 = 0$, алгоритм заканчивает свою работу, и система (3) несовместна.

Пусть на $(i-1)-$м шаге построено множество T_{i-1} э.к.

i-й шаг индукции. Для всех э.к. U из T_{i-1} формируем множество $T_\Im$ э.к. $\Im = U \cdot B$, где B э.к. в д.н.ф. N_{i+1}^0 и $U \cdot B \neq 0$.

Пусть множество $T_i = \bigvee_{V_\Im; \Im \in T_{i-1}} T_\Im$. Если $T_i = 0$, то алгоритм заканчивает свою работу и система (3) несовместна.

Положим, что после (t-1) – го шага индукции построено множество T_{i-1} э.к. такое, что $T_{i-1} \neq 0$. Отсюда следует, что система (3) совместна[9-10].

Таким образом, общий алгоритм определения совместности подсистемы (2) системы (1), заданной в виде (3), состоит из двух этапов. На первом этапе строим однородно-единичную матрицу $\|a_{ij}\|_{t \times t}$ и переходим ко второму этапу. На втором этапе к системе (3) применяем процедуру ПП.

Приближенный алгоритм поиска.

Пусть $M = \{f_1 = 1,\ f_2 = 1, ..., f_m = 1\}$,

$$a_{ij} = \begin{cases} 1, & \text{если } f_i \cdot f_j \neq 0,\ i,j = \overline{1,m}; \\ 0 - & \text{в противном случае.} \end{cases}$$

Пусть $A_{i_1 i_2 ... i_k}$ - квадратная подматрица матрицы $A = \|a_{ij}\|_{m \times m}$, составленная из элементов a_{ij}, где $i, j = i_1, i_2, ..., i_k$, $1 \leq k \leq m$.

Подматрицу $A_{i_1 i_2 ... i_k}$ не содержащую нулей, назовем максимальной, если любая другая квадратная подматрица, включающая в себя $A_{i_1 i_2 ... i_k}$, не является однородно-единичной матрицей.

Считается, что $A_{i_1 i_2 ... i_k}$ соответствует подмножеству $\{f_{i_1} = 1,\ f_{i_2} = 1, ..., f_{i_k} = 1\}$ на M и задается монотонной функцией $q(y_{i_1}, y_{i_2}, ..., y_{i_k})$.

Алгоритм поиска максимальных совместных подсистем состоит в следующем:

***Этап* I.** Находим все однородно – единичные подматрицы матрицы $\|a_{ij}\|$.

***Этап* II.** Для всех максимальных подматриц $A_{i_1 i_2 ... i_k}$ строим систему $M_{i_1 i_2 ... i_k} = \{f_{i_1} = 1,\ f_{i_2} = 1, ..., f_{i_k} = 1\}$ и, применяя алгоритм A_M, находим м.в.н. монотонной булевой функции, соответствующей $M_{i_1 i_2 ... i_k}$.

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

Обозначим через $\{A\}$ множество всех максимальных однородно-единичных подматриц в $\|a_{ij}\|$.

Пусть $A_{i_1 i_2 \ldots i_k}$ - максимальная подматрица из $\{A\}$ и $q(y_{i_1}, y_{i_2}, \ldots, y_{i_k})$ – монотонная булева функция, соответствующая подсистеме $M_{i_1 i_2 \ldots i_k}$. Множество всех таких булевых функции обозначим через $\tilde{A}$.

Пусть $|\tilde{\alpha}| = \begin{pmatrix} \max|\tilde{\beta}| \\ \tilde{\beta} \text{ м.в.н. } q \in \tilde{A} \end{pmatrix}$. Очевидно, что $\tilde{\alpha}$ есть м.в.н. $q(y_1, y_2, \ldots, y_m)$.

Таким образом, задача поиска м.в.н. $q(y_1, y_2, \ldots, y_m)$ свелась к нахождению м.в.н. всех монотонных булевых функции из $\tilde{A}$.

Приближенный алгоритм строим в два этапа. На первом этапе строим максимальную подматрицу $A_{i_1 i_2 \ldots i_k}$ так, что $k = \begin{pmatrix} \max t \\ A_{i_1 i_2 \ldots i_t} \in \{A\} \end{pmatrix}$.

На втором этапе, применяя алгоритм A_M, ищем м.в.н. $q(y_{i_1}, y_{i_2}, \ldots, y_{i_k})$. Для этого на первом этапе из A удоляем нулевые строки и столбцы с наименьшей нормой. Первый этап состоит на двух подэтапов. На первом выявляется i – я строка и i – й столбец с наименьшим числом единиц. На втором из A удаляем i – ю строку и i – й столбец. Если $A_{i_1 i_2 \ldots i_k}$ - единичная матрица, то алгоритм заканчивает свою работу. В противном случае возвращаемся к первому подэтапу.

3. Решение систем нелинейных булевых уравнений второй степени специального класса

Исследуются отдельные классы систем нелинейных булевых уравнений второй степени, заданных полиномами Жегалкина, которые являются алгебраической моделью S-блоков симметрических алгоритмов шифрования. Рассматриваются некоторые проблемы минимизации специальных дизъюнктивных нормальных форм, полученных от полинома Жегалкина второй степени специальных классов. Предлагается критерий поглощения сложных конъюнкций окрестностью первого порядка конъюнкций высказываний отдельного класса систем нелинейных булевых уравнений второй степени, заданных полиномами Жегалкина

Исследуется специальный класс систем нелинейных булевых уравнений второй степени:

$$\mathrm{R} = \{\mathrm{f}_1(x_1, x_2, \ldots, x_\mathrm{n}) = \alpha_1, \mathrm{f}_2(x_1, x_2, \ldots, x_\mathrm{n}) = \alpha_2, \ldots, \mathrm{f}_\mathrm{m}(x_1, x_2, \ldots, x_\mathrm{n}) = \alpha_\mathrm{m}\}$$

Причем высказывание $\mathrm{f}(x_1, x_2, \ldots, x_\mathrm{n})$ из R имеет вид:

$$f = \sum_{\substack{i,j=k \\ i<j}}^{k+3} a_{ij} x_i x_j \oplus \sum_{\substack{i,j=e \\ i<j}}^{e+3} b_{ij} x_i x_j \oplus \sum_{\substack{i,j=p \\ i<j}}^{p+3} c_{ij} x_i x_j \oplus \sum_{\substack{i,j=q \\ i<j}}^{q+3} d_{ij} x_i x_j \oplus \sum_{i=t}^{t+3} x_i,$$

где $k+3<e,\ e+3<p,\ p+3<q,\ q+3<t,$

$$\sum_{i,j=k}^{k+3} a_{ij} = \sum_{i,j=e}^{e+3} b_{ij} = \sum_{i,j=p}^{p+3} c_{ij} = \sum_{i,j=q}^{q+3} d_{ij} = 4, \{a_{ij}, b_{ij}, c_{ij}, d_{ij}, e_i\} \in \{0,\ 1\}.$$

Здесь знаки $\oplus$, $\sum$ - подразумевается как сумма по mod 2.

Для решения нелинейных булевых уравнений второй степени исследуются вопросы компактного представления высказываний f с помощью группировки элементов, введением новых переменных, преобразование f в специальные д.н.ф. с помощью более оптимальным методом десятичного представления с.к.

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

упрощение специальных д.н.ф. и основные особенности реализации формул для специального класса систем нелинейных булевых уравнений второй степени.

Здесь суммы вида $\sum_{i,j=v}^{v+3} q_{ij}x_ix_j$ и $\sum_{i=w}^{w+1} e_ix_i$ назовем группой элементов высказывания f. Кроме того , группы различных уравнений(высказываний) системы R попарно не совпадает.

Метод решения системы R состоит в компактном представлений f_i с помощью группировки элементов введением новых переменных, преобразованием последних в д.н.ф. и их упрощением. Поиск решений системы R осуществляется с помощью алгоритма решения системы линейных булевых уравнений.

Функционал произвольной системы α, полученный из R группировкой и заменой переменных элементов высказываний, обозначим так:

$\Psi_\alpha=\Sigma\varphi_y$ |Y|, здесь {Y} -множество переменных в системе α, φ_y - число $Y\in\{Y\}$ переменных Y и |Y| - число элементов в Y. Алгоритм группировки системы R из заданного класса состоит в следующем:

выделяются группы элементов высказываний системы R; производятся всевозможные группировки в группах и вводятся новые переменные; из каждой группы выбираются такие группировки элементов, чтобы для полученной системы α функционал Ψ_α был максимальным среди всех функционалов Ψ_β сисем β, сформированных из группировок групп системы. Доказана, что в каждой высказывание $f(x_1, x_2, \ldots, x_n)$ из R в начальном этапе участвует 20 элементарных конъюнкции, а после группировки и введения новых переменных высказывания $F(\tilde{x},Y(\tilde{x}))$ системы R* будут содержать не более 9 ти линейных конъюнкции. Из этих данных по

$U_1 \oplus U_2 \oplus \ldots \oplus U_t = \vee_{\sigma 1\oplus\sigma 2\oplus\ldots\oplus\sigma t=1} U_1^{\sigma_1}\&U_2^{\sigma_2}\&\ldots\&U_t^{\sigma_t}$ имеем $L_k(f)=2^{20}, L_k(F)=2^9$.

Отсюда видно, что разница сложности высказывании f и F сокращается 2^{11} раза, т.е. $L_k=\frac{L_k(f)}{L_k(F)}=\frac{2^{20}}{2^9}=2^{11}$, где $L_k(Q)$ –число элементарных конъюнкций, входящих в Q д.н.ф. имеем

Это означает, что метод группировки элементов и введение новых переменных для уравнений второй степени специального класса 2^{11} раз уменьшает сложность высказываний булевых уравнений.

Для решения этой системы выделяются подсистемы R* с помощью алгоритма окрестности первого порядка и приводятся к виду линейных логических уравнений

$$x_{j_1}^{\sigma'_1}\ x_{j_2}^{\sigma'_2}\ \ldots.\ x_{j_k}^{\sigma'_l}\ Y_{l_i m_i}^{\sigma'_{l+i}} Y_{l_j m_j r_j}^{\sigma'_{l+j}} Y_{l_k m_k r_k s_k}^{\sigma'_{l+k}} = 1, l \le n, i \le 8, j \le 16, k \le 32,$$

и упрощение специальных д.н.ф. с помощью следующих нүлевых тождеств:

а) для линейной формы двух переменных

$$x_i x_j Y_{ij}=0, x_i\bar{x}_j\bar{Y}_{ij}=0, \bar{x}_i x_j\bar{Y}_{ij}=0, \bar{x}_i\bar{x}_j Y_{ij}=0,$$

б) для линейной формы трех переменных

$$x_i x_j x_k\bar{Y}_{ijk}=0,\ x_i x_j\bar{x}_k Y_{ijk}=0,\ x_i\bar{x}_j x_k Y_{ijk}=0,\ x_i x_j x_k Y_{ijk}=0,\ x_i\bar{x}_j\bar{x}_k\bar{Y}_{ijk}=0,$$
$$\bar{x}_i x_j\bar{x}_k\bar{Y}_{ijk}=0, \bar{x}_i\bar{x}_j x_k\bar{Y}_{ijk}=0, \bar{x}_i\bar{x}_j\bar{x}_k Y_{ijk}=0,$$

в) для линейной формы четырех переменных

$$x_i x_j x_k x_l Y_{ijkl}=0, x_i x_j x_k\bar{x}_l\bar{Y}_{ijkl}=0, x_i x_j\bar{x}_k x_l\bar{Y}_{ijkl}=0, x_i\bar{x}_j x_k x_l\bar{Y}_{ijkl}=0, \bar{x}_i x_j x_k x_l\bar{Y}_{ijkl}=0,$$
$$x_i x_j\bar{x}_k\bar{x}_l Y_{ijkl}=0, x_i\bar{x}_j x_k\bar{x}_l Y_{ijkl}=0, \bar{x}_i x_j\bar{x}_k x_l Y_{ijkl}=0, x_i\bar{x}_j\bar{x}_k x_l Y_{ijkl}=0, \bar{x}_i x_j\bar{x}_k x_l Y_{ijkl}=0,$$
$$\bar{x}_i\bar{x}_j x_k x_l Y_{ijkl}=0, \bar{x}_i\bar{x}_j\bar{x}_k x_l\bar{Y}_{ijkl}=0, \bar{x}_i\bar{x}_j x_k\bar{x}_l\bar{Y}_{ijkl}=0, \bar{x}_i x_j\bar{x}_k\bar{x}_l\bar{Y}_{ijkl}=0, x_i\bar{x}_j\bar{x}_k\bar{x}_l\bar{Y}_{ijkl}=0,$$

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

$$\bar{x}_i \bar{x}_j \bar{x}_k \bar{x}_l Y_{ijkl} = 0.$$

Далее сокращаем применяя основные особенности реализации формул для специального класса систем нелинейных булевых уравнений второй степени:

а) для линейной формы двух переменных

$$\bar{x}_i Y_{ij} = \bar{x}_i x_j, x_j \bar{Y}_{ij} = x_i x_j, x_i Y_{ij} = \bar{x}_i x_j, x_i \bar{Y}_{ij} = x_i x_j, x_i Y_{ij} = x_i \bar{x}_j,$$

$$\bar{x}_i Y_{ij} = x_i \bar{x}_j, \bar{x}_j \bar{Y}_{ij} = \bar{x}_i \bar{x}_j, x_i x_j \bar{Y}_{ij} = x_i x_j, \bar{x}_i x_j Y_{ij} = \bar{x}_i x_j,$$

$$x_i \bar{x}_j Y_{ij} = x_i \bar{x}_j, \bar{x}_i \bar{x}_j \bar{Y}_{ij} = \bar{x}_i \bar{x}_j,$$

б) для линейной формы с тремя переменными

$$x_i x_j x_k Y_{ijk} = x_i x_j x_k, x_i x_j \bar{x}_k \bar{Y}_{ijk} = x_i x_{jk}, x_i \bar{x}_j x_k \bar{Y}_{ijk} = x_i \bar{x}_j x_k, \bar{x}_i x_j x_k \bar{Y}_{ijk} = \bar{x}_i x_j x_k,$$

$$x_i \bar{x}_j \bar{x}_k Y_{ijk} = x_i \bar{x}_j \bar{x}_k, \bar{x}_i x_j \bar{x}_k Y_{ijk} = \bar{x}_i x_j \bar{x}_k, \bar{x}_i \bar{x}_j x_k Y_{ijk} = \bar{x}_i \bar{x}_j x_k, \bar{x}_i \bar{x}_j \bar{x}_k \bar{Y}_{ijk} = \bar{x}_i \bar{x}_j \bar{x}_k.$$

в) для линейной формы четырех переменных:

$$x_i x_j x_k x_l \bar{Y}_{ijkl} = x_i x_j x_k x_l, x_i x_j x_k \bar{x}_l Y_{ijkl} = x_i x_j x_k \bar{x}_l, x_i x_j \bar{x}_k x_l Y_{ijkl} = x_i x_j \bar{x}_k x_l,$$

$$x_i \bar{x}_j x_k x_l Y_{ijkl} = x_i \bar{x}_j x_k x_l, \bar{x}_i x_j x_k x_l \bar{Y}_{ijkl} = \bar{x}_i x_j x_k x_l, x_i x_j \bar{x}_k \bar{x}_l \bar{Y}_{ijkl} = x_i x_j \bar{x}_k \bar{x}_l,$$

$$x_i \bar{x}_j x_k \bar{x}_l \bar{Y}_{ijkl} = x_i \bar{x}_j x_k \bar{x}_l, \bar{x}_i x_j x_k \bar{x}_l \bar{Y}_{ijkl} = \bar{x}_i x_j x_k \bar{x}_l, x_i \bar{x}_j \bar{x}_k x_l \bar{Y}_{ijkl} = x_i \bar{x}_j \bar{x}_k x_l,$$

$$\bar{x}_i x_j \bar{x}_k x_l \bar{Y}_{ijkl} = \bar{x}_i x_j \bar{x}_k x_l, \bar{x}_i \bar{x}_j x_k x_l \bar{Y}_{ijkl} = \bar{x}_i \bar{x}_j x_k x_l, \bar{x}_i \bar{x}_j \bar{x}_k x_l Y_{ijkl} = \bar{x}_i \bar{x}_j \bar{x}_k x_l,$$

$$\bar{x}_i \bar{x}_j x_k \bar{x}_l Y_{ijkl} = \bar{x}_i \bar{x}_j x_{kl}, \bar{x}_i x_j \bar{x}_k \bar{x}_l Y_{ijkl} = \bar{x}_i x_j \bar{x}_k \bar{x}_l, x_i \bar{x}_j \bar{x}_k \bar{x}_l Y_{ijkl} = x_i \bar{x}_j \bar{x}_k \bar{x}_l,$$

и получаем совокупность уравнений вида $x_{i_1}^{\sigma_1} x_{i_2}^{\sigma_2} \& \ldots \& x_{i_k}^{\sigma_k} = 1,$ для каждого из которых выписываем решение $\bar{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n),$ где

$$\alpha_\gamma = \begin{cases} \sigma_\gamma, \textit{если } \gamma \in (i_1, i_2, \ldots, i_k), \\ *, \textit{в противном случае.} \end{cases}$$

Заключение

Проведено исследование методов поиска максимальных совместных подсистем систем нелинейных булевых уравнений. Разработан алгоритм поиска максимальных подсистем систем булевых уравнений на основе решения задачи расшифровки и поиска максимального верхнего нуля монотонных булевых функций. Дано решение систем нелинейных булевых уравнений второй степени специального класса. Практическое значимость результатов исследований заключается в возможности решения систем специальных нелинейных булевых уравнений второй степени на основе группирования и минимизации логических высказываний в классе д.н.ф., которые являются алгебраической моделью S-блоков симметрических алгоритмов шифрования.

Список использованных литературы:

[1]. Кабулов В.К., Кабулов А.В., Норматов И.Х. Логические методы алгоритмизации в теории управляющих систем. Монография: Германия.2018, Изд. “Ламберт” С.191.

[2]. Kabulov A.V., Berdimurodov M.A., Saymanov I.M. Kriptografik algoritm mikrobuyruqlarining mantiqiy bul funksiya shakli (AES, EL-GAMAL) //2021, No. 3 (127/1). – 2023. – Т. 127. – №. 101. – С. 5-16.

[3]. Berdimurodov M., Baizhumanov A. Algorithms for minimizing functions of the algebra of logic in the class of disjunctive normal forms and estimating their complexity //2022

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118

International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2022. – С. 1-5.
[4]. Mendelson E. Introduction to mathematical logic. Fifth edition. – NY.: «Chapman&Hall/CRC», 2010.
[5]. Гиндикин С.Г. Алгебра логики в задачах. - М.: «Наука», 1972.
[6]. Ершов Ю.Л., Палютин Е.А. Математическая логика. - М.: «Наука», 2011.
[7]. Игошин В.И. Математическая логика и теория алгоритмов. -М.: «Наука», 2008.
[8]. Клини С.К. Математическая логика. - М.: «Мир», 1973.
[9]. Новиков П.С. Элементы математической логики. - М.: «Наука», 1973.
[10]. Bhattacharya P.B., 1995 etc Basic Abstract Algebra, 2nd edition, Cambridge University Press.

© Journal of Advances in Engineering Technology Vol.4(16), October – December, 2024
DOI 10.24412/2181-1431-2024-4-110-118