УДК 519.7

РЕАЛИЗАЦИЯ ТИПОВЫХ ФУНКЦИЙ ГИБРИДНЫХ КРИПТОСИСТЕМ АРИФМЕТИКО-ЛОГИЧЕСКИМИ ПОЛИНОМАМИ

А.К. Вишневский, адъюнкт, e-mail: vishn.artem@yandex.ru
О.А. Финько, профессор, e-mail: ofinko@yandex.ru
Краснодарское высшее военное училище (ВИ)

Представлен метод устранения противоречия между показателями сложности и временными характеристиками асимметрических и симметрических криптоалгоритмов, входящих в состав гибридных криптосистем, путем применения числовых способов представления функций алгебры логики для реализации типовых криптографических примитивов.

Ключевые слова: *реализация криптографических алгоритмов, операция подстановки, параллельные логические вычисления, числовая нормальная форма, арифметико-логические формы, модулярная арифметика.*

STANDARD FUNCTION HYBRID CRYPTOSYSTEM ARITHMETIC AND LOGICAL MULTINOMIAL REALIZATION

A.K. Vishnevsky, adjunct, e-mail: vishn.artem@yandex.ru
O.A. Finko, professor, e-mail: ofinko@yandex.ru
Krasnodar High Military School (VI)

In the article method eliminating the contradiction between factor of the difficulties and temporary feature asymmetric and symmetrical cryptographic algorithm is discussed. This method is founded on using the numeric ways of the function algebras of the logic.

Key words: *cryptographic algorithm realization, substitution operation, parallel Boolean calculations, numeric normal form, arithmetic and logical forms, modular arithmetic.*

Введение

Для решения задач шифрованной связи широкое применение в настоящее время получили так называемые гибридные криптосистемы, представляющие собой совокупность асимметрической (двухключевой) и симметрической (одноключевой) криптосистем (АКС, СКС). При этом АКС используется для выработки секретного ключа и обеспечивает, таким образом, функционирование СКС.

Анализ временных и вычислительных затрат, связанных с реализацией этих двух различных криптосистем, выявил следующее противоречие. Для обеспечения секретным ключом, по крайней мере, одного сеанса связи АКС функционирует однократно в течение короткого (по сравнению с длительностью сеанса) интервала времени. Остальное время сеанса связи посвящено собственно передаче секретной информации на секретных ключах с применением СКС.

В то же время, если проанализировать вычислительные затраты, связанные с реализацией обеих типов криптосистем, выявится обратная картина: АКС требует значительно более высоких вычислительных ресурсов по сравнению с затратами, необходимыми для реализации СКС. Это связано с тем, что, как правило, алгоритм, лежащий в основе АКС, требует реализации экспоненциальной функции в конечном целочисленном кольце, оперируя при этом многоразрядными (более тысячи) данными. СКС оперирует, как правило, 32- и 64-разрядными данными при реализации операций в конечном целочисленном кольце (как правило, по модулю $2^n \pm 1$) и преимущественно операций, легко представляемых аппаратом алгебры логики (подстановки, сдвиги, конкатенации, нелинейные функции усложнения и пр.).

Таким образом, налицо противоречие: АКС, которая требует от технических средств максимальных вычислительных ресурсов, используется однократно и значительное время попросту простаивает; СКС, поддерживающая непосредственно весь сеанс связи, значительно менее требовательна к мощностным характеристикам специальных вычислительных средств.

Устранение данного противоречия возможно следующим образом. В настоящее время

определенное развитие получило новое направление в области реализации функций алгебры логики (ФАЛ): реализация ФАЛ посредством арифметико-логических [1, 2], в частности модулярных [3] форм, то есть путем выполнения арифметических операций. Таким образом, данный математический аппарат позволяет реализовать типовые ФАЛ, лежащие в основе СКС, посредством типовых арифметических операций, используемых при реализации АКС. Так как АКС и СКС в составе гибридной криптосистемы используются последовательно, то возникает возможность реализовать обе криптосистемы единым математическим аппаратом (теория арифметико-логических форм) и единым техническим средством, реализующим многоразрядные операции в кольце целых чисел.

1. Представление подстановки в терминах алгебры логики

Анализ различных СКС выявил, что большинство из них построено на основе типовых числовых и логических операций и функций (см. табл. 1: здесь $\bar{\oplus}$ – векторная операции сложения по модулю 2; $\boxplus$, $\boxminus$ и $\otimes$ – соответственно операции сложения, вычитания и умножения по модулю $(2^n - i)$, $i \in \{0,1\}$, $n \in N$; $<<<>>>$ – циклический сдвиг (влево, вправо) на i разрядов; $||$ – конкатенация; S – система подстановок; P – перестановка).

Таблица 1

Типовые операции симметрических шифров

	GOST	*Kasumi*	*Blowfish*	*IDEA*	*CAST*	*SAFER*	*Misty*	*Camellia*	*SEAL*
$\bar{\oplus}$	$\bar{\oplus}$ 32 bit	$\bar{\oplus}$ 7,9 bit	$\bar{\oplus}$ 32 bit	$\bar{\oplus}$ 16 bit	$\bar{\oplus}$ 16 bit	$\bar{\oplus}$ 8 bit	$\bar{\oplus}$ 7,9 bit	$\bar{\oplus}$ 64 bit	$\bar{\oplus}$ 32 bit
$<<<>>>$	$11<<<$	$i<<<$			$i<<<$		$i<<<$	$1<<<$	$1<<<$ $>>>1$
$\boxplus$	2^{32} $2^{32}-1$		2^{32}	2^{16}	2^{16}	2^8			
$\boxminus$					$2^{16}-1$				
$\|\|$	$32\|\|32$	$7\|\|9$ $\|\|$ $7\|\|9$	$32\|\|32$	$64\|\|64$	$16\|\|16$ $\|\|$ $16\|\|16$	$64\|\|64$ $\|\|$ $64\|\|64$	$7\|\|9$ $\|\|$ $7\|\|9$	$64\|\|64$	
S	4×4	7×7 9×9	8×32		8×16	8×8	7×7 9×9	8×8	
P						16×16		2×2	
$\otimes$				$2^{16}-1$					

Операция подстановки степени $k = 2^{\log k}$ используется в большинстве современных блочных шифров (табл. 1), поэтому имеет смысл рассмотреть особенности ее числовой реализации.

Подстановка – это взаимно однозначное отображение конечного множества в себя. При соответствующей нумерации (или упорядочении) элементов конечного множества, на котором определена подстановка, ее можно свести к подстановке на некотором конечном подмножестве натуральных чисел:

$$\sigma_t = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma_t^{(1)} & \sigma_t^{(2)} & \dots & \sigma_t^{(k)} \end{pmatrix}, \qquad (1)$$

где $\sigma_t^{(i)}, i \in \{1,2,\dots,k\}$; $\sigma_t^{(i)} \neq \sigma_t^{(j)}$, $i \neq j$.

Система подстановок имеет вид

$$\sigma = \begin{cases} \sigma_1 = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma_1^{(1)} & \sigma_1^{(2)} & \dots & \sigma_1^{(k)} \end{pmatrix}, \\ \sigma_2 = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma_2^{(1)} & \sigma_2^{(2)} & \dots & \sigma_2^{(k)} \end{pmatrix}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \sigma_s = \begin{pmatrix} 1 & 2 & \dots & k \\ \sigma_s^{(1)} & \sigma_s^{(2)} & \dots & \sigma_s^{(k)} \end{pmatrix}. \end{cases} \qquad (2)$$

Тогда вектор булевых значений, принимаемых $\sigma_t\left(t\in\{1,2,...,s\}\right)$ (табл. 2), обозначим как

$$\vec{\sigma}_t=\left[\, f_t^{(1)}\left(\vec{x}_t\right) f_t^{(2)}\left(\vec{x}_t\right)...f_t^{(\log k)}\left(\vec{x}_t\right)\right], \qquad (3)$$

где $f_t^{(i)}\left(\vec{x}_t\right)$ – ФАЛ, определенная на векторе существенных булевых переменных $\vec{x}_t=\left[\, x_t^{(1)}x_t^{(2)}...x_t^{(\log k)}\right]$.

Таблица 2

Таблица истинности σ_t

№	$x_t^{(1)}$	$x_t^{(2)}$	...	$x_t^{(\log k)}$	σ_t	$f_t^{(1)}$	$f_t^{(2)}$	…	$f_t^{(\log k)}$
1	0	0	…	0	$\sigma_t^{(1)}$	$f_t^{(1)}\left(\vec{x}_t^{(1)}\right)$	$f_t^{(2)}\left(\vec{x}_t^{(1)}\right)$	…	$f_t^{(\log k)}\left(\vec{x}_t^{(1)}\right)$
2	0	0	…	1	$\sigma_t^{(2)}$	$f_t^{(1)}\left(\vec{x}_t^{(2)}\right)$	$f_t^{(2)}\left(\vec{x}_t^{(2)}\right)$	…	$f_t^{(\log k)}\left(\vec{x}_t^{(2)}\right)$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
k	1	1	…	1	$\sigma_t^{(k)}$	$f_t^{(1)}\left(\vec{x}_t^{(k)}\right)$	$f_t^{(2)}\left(\vec{x}_t^{(k)}\right)$	…	$f_t^{(\log k)}\left(\vec{x}_t^{(k)}\right)$

Соответственно, вектор системы (2) подстановок (табл. 3) $\vec{\sigma}=\left[\vec{\sigma}_1\vec{\sigma}_2...\vec{\sigma}_s\right]$, $\vec{x}=\left[\vec{x}_1\ \vec{x}_2\ ...\ \vec{x}_s\right]$, где $\vec{\sigma}$ интерпретируется как система ФАЛ:

$$F\left(\vec{x}_1,\vec{x}_2,...,\vec{x}_s\right)=F(\vec{x})=\begin{cases} f_1^{(1)}\left(\vec{x}_1\right), \\ ..... \\ f_1^{(\log k)}\left(\vec{x}_1\right), \\ ..... \\ f_s^{(1)}\left(\vec{x}_s\right), \\ ..... \\ f_s^{(\log k)}\left(\vec{x}_s\right); \end{cases} \qquad (4)$$

при этом лексикографический порядок упорядоченных существенных переменных $\vec{x}=$ $=\left[x_1^{(1)}...\,x_1^{(\log k)}...\,x_s^{(1)}...\,x_s^{(\log k)}\right]$ сохраняется для каждой σ_t в отдельности.

Таблица 3

Таблица истинности системы подстановок σ

№	$\vec{x}_1$	$\vec{x}_2$	…	$\vec{x}_s$	$\sigma_1\left(\vec{x}_1\right)$	$\sigma_2\left(\vec{x}_2\right)$	…	$\sigma_s\left(\vec{x}_s\right)$	$\sigma(\vec{x})$
1	$\vec{x}_1^{(1)}$	$\vec{x}_2^{(1)}$	…	$\vec{x}_s^{(1)}$	$\sigma_1^{(1)}\left(\vec{x}_1^{(1)}\right)$	$\sigma_2^{(1)}\left(\vec{x}_2^{(1)}\right)$	…	$\sigma_s^{(1)}\left(\vec{x}_s^{(1)}\right)$	$\sigma^{(1)}\left(\vec{x}^{(1)}\right)$
2	$\vec{x}_1^{(2)}$	$\vec{x}_2^{(2)}$	…	$\vec{x}_s^{(2)}$	$\sigma_1^{(2)}\left(\vec{x}_1^{(2)}\right)$	$\sigma_2^{(2)}\left(\vec{x}_2^{(2)}\right)$	…	$\sigma_s^{(2)}\left(\vec{x}_s^{(2)}\right)$	$\sigma^{(2)}\left(\vec{x}^{(2)}\right)$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
k	$\vec{x}_1^{(k)}$	$\vec{x}_2^{(k)}$	…	$\vec{x}_s^{(k)}$	$\sigma_1^{(k)}\left(\vec{x}_1^{(k)}\right)$	$\sigma_2^{(k)}\left(\vec{x}_2^{(k)}\right)$	…	$\sigma_s^{(k)}\left(\vec{x}_s^{(k)}\right)$	$\sigma^{(k)}\left(\vec{x}^{(k)}\right)$

2. Представление системы ФАЛ в числовой нормальной форме

Существуют различные способы реализации систем ФАЛ [4-6]. Определенные преимущества имеет представление в числовой нормальной форме [7].

Представим $f_t^{(j)}\left(\vec{x}_t\right)$ (табл. 2) в числовой нормальной форме или числовым полиномом (ЧП):

$$P_t^{(j)}\left(\vec{x}_t\right)=\sum_{i=1}^{k}a_{i-1}x_{t,1}^{i_1}x_{t,2}^{i_2}...x_{t,\log k}^{i_{\log k}}, \qquad (5)$$

где $a_j \in Z$, $i_j \in \{0,1\}$, $\left(i_1\ i_2\ \ldots\ i_{\log k}\right)_2 = \sum_{j=1}^{\log k} 2^{\log k - j} i_j \left(i_j \in \{0,1\}\right)$, $x_{t,j}^{i_j} = \begin{cases} x_{t,j}, & i_j = 1, \\ 1, & i_j = 0. \end{cases}$

Тогда подсистема ФАЛ (3), соответствующая подстановке σ_t, может быть реализована ЧП:

$$N_t = D_t\left(\vec{x}_t\right) = \sum_{j=1}^{\log k} 2^{j-1} P_t^{(j)}\left(\vec{x}_t\right) = \sum_{i=1}^{k} c_{i-1} x_{t,1}^{i_1} x_{t,2}^{i_2} \ldots x_{t,\log k}^{i_{\log k}}, \quad (6)$$

где $c_j \in Z$. При этом результат вычисления (6) число $N_t = \left(n_{t,1}\ n_{t,2}\ \ldots n_{t,\log k}\right)_2$ интерпретируется как вектор ФАЛ $\left[f_t^{(\log k)}\left(\vec{x}_t\right) f_t^{(\log k-1)}\left(\vec{x}_t\right) \ldots f_t^{(1)}\left(\vec{x}_t\right)\right]$.

Наконец, система (2) посредством (3) может быть реализована ЧП:

$$N = H(\vec{x}) = \sum_{t=1}^{s} 2^{(t-1)\log k} D_t\left(\vec{x}_t\right) = \sum_{\substack{i=1,\ldots,k \\ t=1,\ldots,s}} d_{t,i-1} x_{t,1}^{i_1} x_{t,2}^{i_2} \ldots x_{t,\log k}^{i_{\log k}} \left(\mathrm{mod}\ 2^{s\log k}\right), \quad (7)$$

где $d_{t,j} \in Z_{2^{s\log k}}$, где $N = \left(n_1 n_2 \ldots n_{s\log k}\right)_2$ – представление числа N в двоичной системе счисления, в котором значения разрядов $n_1, n_2, \ldots, n_{s\log k}$ являются результатом вычисления ФАЛ: $f_s^{(\log k)}(\vec{x}_s), \ldots, f_s^{(1)}\left(\vec{x}_s\right), \ldots, f_1^{(\log k)}\left(\vec{x}_1\right), \ldots, f_1^{(1)}\left(\vec{x}_1\right)$.

3. Алгоритм построения ЧП для системы подстановок

Реализацию системы подстановок (2) ЧП можно свести к строгой последовательности действий, которую, в свою очередь, можно реализовать программно-аппаратными средствами.

Шаг 1. Формализация исходных данных – построение таблицы истинности (табл. 3) и построение вектора истинности: $\vec{Y}_t = \left[Y_t^{(1)} Y_t^{(2)} \ldots Y_t^{\left(2^{\log k}\right)} \right]^{\mathrm{T}}$, где $Y_t^{(i)} \in Z$, $Y_t^{(i)} = \sum_{j=1}^{\log k} 2^{j-1} y_{t,i}^{(j)} \left(y_{t,i}^{(j)} \in \{0,1\}\right)$.

Шаг 2. Вычисление коэффициентов ЧП (6) $\vec{c}_t = \mathbf{A}_{\mathbf{2}^{\log k}} \vec{Y}_t$, где $\vec{c}_t = \left[c_{t,0} c_{t,1} \ldots c_{t,2^{\log k}-1} \right]^T$ – вектор коэффициентов (6) (арифметический спектр ФАЛ [3]), T – символ транспонирования. Матрица $\mathbf{A}_{\mathbf{2}^{\log k}} = \begin{bmatrix} \mathbf{A}_{\mathbf{2}^{\log k-1}} & 0 \\ -\mathbf{A}_{\mathbf{2}^{\log k-1}} & \mathbf{A}_{\mathbf{2}^{\log k-1}} \end{bmatrix}$ является $\log k$-й кронекеровской степенью $\mathbf{A}_{\mathbf{2}^{\log k}} = \bigotimes_{i=1}^{\log k} \mathbf{A}_1$ базовой матрицы $\mathbf{A}_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$.

Шаг 3. Получение ЧП для подстановки (1):

$$D_t\left(\vec{x}_t\right) = \begin{bmatrix} c_{t,0} \\ c_{t,1} \\ c_{t,2} \\ c_{t,3} \\ \ldots \\ c_{t,2^{\log k}-1} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x_{t,\log k} \\ x_{t,\log k-1} \\ x_{t,\log k-1} x_{t,\log k} \\ \ldots \\ x_{t,1} x_{t,2} \ldots x_{t,\log k} \end{bmatrix} \left(\mathrm{mod}\ 2^{\log k}\right) = \sum_{i=1}^{2^{\log k}} c'_{t,i-1} x_{t,1}^{i_1} x_{t,2}^{i_2} \ldots x_{t,\log k}^{i_{\log k}} \left(\mathrm{mod}\ 2^{\log k}\right),$$

где $c'_{t,j} = c_{t,j} \left(\mathrm{mod}\ 2^{\log k}\right)$.

Шаг. 4. Получение ЧП для системы подстановок (2):

$$H(\vec{x}) = \sum_{t=1}^{s} 2^{s-1} D_t\left(\vec{x}_t\right) = \sum_{\substack{i=1,\ldots,k \\ t=1,\ldots,s}} d_{t,i-1} x_{t,1}^{i_1} x_{t,2}^{i_2} \ldots x_{t,\log k}^{i_{\log k}} \left(\mathrm{mod}\ 2^{s\log k}\right).$$

4. Оценка ЧП

Оценку числового полинома будем производить на примере реализации блока подстановок ГОСТ 28.147-89 (Приложение А). Верхняя граница сложности ЧП L системы подстановок (2) от $s\log k$ переменных равна $L = s\left(2^{\log k} - 1\right) + 1$, что для ГОСТ 28.147-89 составляет $L = 8\left(2^4 - 1\right) + 1$. Но в то же время верхняя граница сложности модулярного ЧП L_1 для системы произвольных ФАЛ от того же количества переменных равна $L_1 = 2^{s\log k} = 2^{32} = 4292967296$. То есть при равных количествах переменных в частном и общем случаях выигрыш в сложности ЧП составляет $\frac{L_1}{L} = \frac{4292967296}{121} \approx 35495597$ раз.

В статье был рассмотрен случай решения задачи реализации систем ФАЛ, достаточно «неудобных» для любого способа реализации. На практике для реализации конкретных классов

ФАЛ выбирают соответствующие формы (базисы) представления, которые позволяют получить требуемый выигрыш по выбранным показателям качества (минимальность, тестируемость схемы, надежность реализации и пр.). Поэтому ясно, что при выборе предлагаемого числового способа реализации вначале следует определить класс ФАЛ, позволяющих, при этом, получить какой-либо положительный эффект. С другой стоны, также ясно, что предложенное решение позволяет задействовать достаточно мощное оборудование процессора, которое ранее по этому назначению не использовалось и попросту простаивало. Поэтому по крайней мере можно предполагать некоторый выигрыш в производительности или аппаратурным затратам за счет более рационального использования оборудования или за счет использования дополнительного оборудования в целях увеличения загрузки криптопроцессора и распараллеливания вычислений. Следует упомянуть и о новых открывающихся возможностях: 1) повышения достоверности вычислений, имеющей большое значение для обеспечения безопасности функционирования криптопроцессора, за счет применения избыточных арифметических кодов для контроля ошибок криптографических преобразований и 2) применения высокоэффективных процессоров цифровой обработки сигналов, реализующих теоретико-числовые преобразования, по новому назначению - реализации ФАЛ криптоалгоритмов.

Литература

1. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов / В.Д. Малюгин. – М. : ФИЗМАТЛИТ, 1997. – 192 с.

2. *Yanushkevich S.* Logic design of nanoICs / S. Yanushkevich, V. Shmerko, S. Lyshevski. – CRC Press, 2005.

3. *Финько О.А.* Модулярная арифметика параллельных логических вычислений : монография / О.А. Финько ; под ред. В.Д. Малюгина. – М. : Ин-т проблем управления им. В.А. Трапезникова РАН, 2003. – 224 с. : ил.
http://www.computermuseam.ru/books/archiv/sokcon26.pdf.

4. *Закревский А.Д.* Полиномиальная реализация частичных булевых функций и систем / А.Д. Закревский, Н.Р. Торопов / Изд. 2-е, стереотипное. – М.: Едиториал УРСС, 2003. – 200 с.

5. *Вишневский А.К.* Реализация дискретных криптографических функций линейными числовыми полиномами / А.К. Вишневский, О.А. Финько // 29 Всероссийская ВНТК, г. Серпухов, 2010.

6. Криптографические методы защиты информации : коллективная монография. Сер. Защита информации, кн. 4, гл. : 5–7 / под ред. Е.М. Сухарева. – М. : Радиотехника, 2007. – 312 с.

7. *Логачев О.А.* Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М. : МЦНМО, 2004.

8. *Шнайер Б.* Прикладная криптография / Б. Шнайер / Протоколы, алгоритмы, исходные тексты на Си. – М. : ТРИУМФ, 2003. – 816 с.

Статья поступила в редакцию 01.09.2010 г.

Приложение А

Пример реализации блока подстановок шифра ГОСТ 28.147-89. Значения подстановок взяты из [8] (табл. А1). Для наглядности значения подстановок, коэффициенты и модуль ЧП записаны в 16-ричной системе счисления.

Таблица А1

Значения подстановок ГОСТ 28.147-89

№	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
σ_1	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3
σ_2	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9
σ_3	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B
σ_4	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3
σ_5	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2
σ_6	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E
σ_7	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C
σ_8	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C

Построение ЧП (6) для каждой подстановки:

$$D_1(\vec{x}_1) = (2)_{16}x_1 - (\mathrm{A})_{16}x_1x_3 - x_1x_4 - (12)_{16}x_2x_3 - (\mathrm{B})_{16}x_2x_4 - (\mathrm{C})_{16}x_3x_4 -$$

$$-(8)_{16}x_1x_2+(9)_{16}x_2+(5)_{16}x_3+(6)_{16}x_4+(15)_{16}x_1x_2x_3+(\mathrm{E})_{16}x_1x_2x_3+$$
$$+(\mathrm{D})_{16}x_1x_3x_4+(20)_{16}x_2x_3x_4-(30)_{16}x_1x_2x_3x_4+(4)_{16},$$

$$D_2(\vec{x}_2)=(6)_{16}x_5x_6+(10)_{16}x_5x_7+(4)_{16}x_5x_8+(13)_{16}x_6x_7+(\mathrm{A})_{16}x_6x_8+(\mathrm{B})_{16}x_7x_8-$$
$$-(\mathrm{C})_{16}x_5-(8)_{16}x_6-(\mathrm{A})_{16}x_7-(3)_{16}x_8-(14)_{16}x_5x_6x_7-(17)_{16}x_5x_7x_8-$$
$$-(17)_{16}x_6x_7x_8+(1\mathrm{C})_{16}x_5x_6x_7x_8+(\mathrm{E})_{16},$$

$$D_3(\vec{x}_3)=(2)_{16}x_9x_{11}-(\mathrm{D})_{16}x_9x_{10}-(2)_{16}x_9x_{12}-(2)_{16}x_{10}x_{11}-(\mathrm{A})_{16}x_{10}x_{12}+$$
$$+(9)_{16}x_{11}x_{12}+(9)_{16}x_9+(5)_{16}x_{10}-(4)_{16}x_{11}+(3)_{16}x_{12}+(7)_{16}x_9x_{10}x_{11}+$$
$$+(3)_{16}x_9x_{10}x_{12}-(\mathrm{F})_{16}x_9x_{11}x_{12}-(4)_{16}x_{10}x_{11}x_{12}++(12)_{16}x_9x_{10}x_{11}x_{12}+(5)_{16},$$

$$D_4(\vec{x}_4)=(4)_{16}x_{13}x_{14}-(\mathrm{B})_{16}x_{13}x_{15}-(10)_{16}x_{13}x_{16}+(6)_{16}x_{14}x_{15}+(2)_{16}x_{14}x_{16}-$$
$$-(\mathrm{F})_{16}x_{15}x_{16}+(7)_{16}x_{13}-(7)_{16}x_{14}+(3)_{16}x_{15}+(6)_{16}x_{16}-(4)_{16}x_{13}x_{14}x_{15}-$$
$$-x_{13}x_{14}x_{16}+(1\mathrm{F})_{16}x_{13}x_{15}x_{16}++(\mathrm{D})_{16}x_{14}x_{15}x_{16}-(16)_{16}x_{13}x_{14}x_{15}x_{16}+(7)_{16},$$

$$D_5(\vec{x}_5)=(4)_{16}x_{17}x_{19}-(3)_{16}x_{17}x_{18}+(7)_{16}x_{18}x_{19}+(4)_{16}x_{18}x_{20}-(\mathrm{C})_{16}x_{19}x_{20}-$$
$$-(2)_{16}x_{17}-x_{18}+x_{19}+(6)_{16}x_{20}-x_{17}x_{18}x_{19}-(7)_{16}x_{17}x_{18}x_{20}+$$
$$+(\mathrm{B})_{16}x_{17}x_{19}x_{20}-(3)_{16}x_{18}x_{19}x_{20}-(8)_{16}x_{17}x_{18}x_{19}x_{20}+(6)_{16},$$

$$D_6(\vec{x}_6)=(3)_{16}x_{21}x_{22}-x_{21}x_{23}-(4)_{16}x_{21}x_{24}-(\mathrm{C})_{16}x_{22}x_{23}-(\mathrm{C})_{16}x_{22}x_{24}-$$
$$-(11)_{16}x_{23}x_{24}-x_{21}+(3)_{16}x_{22}+(6)_{16}x_{23}+(7)_{16}x_{24}+(\mathrm{D})_{16}x_{21}x_{22}x_{23}+$$
$$+(\mathrm{C})_{16}x_{21}x_{22}x_{24}+(\mathrm{B})_{16}x_{21}x_{23}x_{24}+(22)_{16}x_{22}x_{23}x_{24}-(20)_{16}x_{21}x_{22}x_{23}x_{24}+(4)_{16},$$

$$D_7(\vec{x}_7)=(10)_{16}x_{25}x_{26}+(17)_{16}x_{25}x_{27}+(\mathrm{C})_{16}x_{25}x_{28}+(\mathrm{B})_{16}x_{26}x_{27}+(\mathrm{E})_{16}x_{26}x_{28}-$$
$$-x_{27}x_{28}-(\mathrm{D})_{16}x_{25}-(\mathrm{A})_{16}x_{26}-(9)_{16}x_{27}-(2)_{16}x_{28}-(1\mathrm{D})_{16}x_{25}x_{26}x_{27}-$$
$$-(16)_{16}x_{25}x_{26}x_{28}-(10)_{16}x_{25}x_{27}x_{28}-(7)_{16}x_{26}x_{27}x_{28}+(20)_{16}x_{25}x_{26}x_{27}x_{28}+(\mathrm{D})_{16},$$

$$D_8(\vec{x}_8)=(8)_{16}x_{29}-(12)_{16}x_{29}x_{31}-(15)_{16}x_{29}x_{32}-(7)_{16}x_{30}x_{31}-(\mathrm{C})_{16}x_{30}x_{32}-$$
$$-(1\mathrm{B})_{16}x_{31}x_{32}-(7)_{16}x_{29}x_{30}+(4)_{16}x_{30}+(\mathrm{C})_{16}x_{31}+(\mathrm{E})_{16}x_{32}+(\mathrm{F})_{16}x_{29}x_{30}x_{31}+$$
$$+(18)_{16}x_{29}x_{30}x_{32}+(2\mathrm{D})_{16}x_{29}x_{31}x_{32}+(13)_{16}x_{30}x_{31}x_{32}-(26)_{16}x_{29}x_{30}x_{31}x_{32}+(1)_{16}.$$

где $\vec{x}_1=(x_1,x_2\,x_3,x_4)$, $\vec{x}_2=(x_5,x_6,x_7,x_8)$, $\vec{x}_3=(x_9,x_{10},x_{11},x_{12})$, $\vec{x}_4=(x_{13},x_{14},x_{15},x_{16})$, $\vec{x}_5=(x_{17},x_{18},x_{19},x_{20})$, $\vec{x}_6=(x_{21},x_{22},x_{23},x_{24})$, $\vec{x}_7=(x_{25},x_{26},x_{27},x_{28})$, $\vec{x}_8=(x_{29},x_{30},x_{31},x_{32})$.

Построение общего ЧП (7) для восьми подстановок:

$$H(\vec{x})=(2)_{16}x_1-(\mathrm{A})_{16}x_1x_3-x_1x_4-(12)_{16}x_2x_3-(\mathrm{B})_{16}x_2x_4-(\mathrm{D})_{16}x_3x_4-$$
$$-(8)_{16}x_1x_2+(9)_{16}x_2+(5)_{16}x_3+(6)_{16}x_4+(15)_{16}x_1x_2x_4+(\mathrm{E})_{16}x_1x_2x_3+$$
$$+(13)_{16}x_1x_3x_4+(20)_{16}x_2x_3x_4-(30)_{16}x_1x_2x_3x_4+(60)_{16}x_5x_6+$$
$$+\left(10^2\right)_{16}x_5x_7+(40)_{16}x_5x_8+(130)_{16}x_6x_7+(\mathrm{A}0)_{16}x_6x_8+(\mathrm{B}0)_{16}x_7x_8-$$
$$-(\mathrm{C}0)_{16}x_5-(80)_{16}x_6-(\mathrm{A}0)_{16}x_7-(30)_{16}x_8-(140)_{16}x_5x_6x_7-$$
$$-(130)_{16}x_5x_7x_8-(170)_{16}x_6x_7x_8+(1\mathrm{C}0)_{16}x_5x_6x_7x_8+\left(2\cdot10^2\right)_{16}x_9x_{11}-$$
$$-\left(\mathrm{D}\cdot10^2\right)_{16}x_9x_{10}-\left(2\cdot10^2\right)_{16}x_9x_{12}-\left(2\cdot10^2\right)_{16}x_{10}x_{11}-$$
$$-\left(\mathrm{A}\cdot10^2\right)_{16}x_{10}x_{12}+\left(9\cdot10^2\right)_{16}x_9+\left(5\cdot10^2\right)_{16}x_{10}-\left(4\cdot10^2\right)_{16}x_{11}+$$

$$+(9\cdot10^2)_{16}\,x_{11}x_{12}+(3\cdot10^2)_{16}\,x_{12}+(7\cdot10^2)_{16}\,x_9x_{10}x_{11}+(3\cdot10^2)_{16}\,x_9x_{10}x_{12}-$$
$$-(\mathrm{F}\cdot10^2)_{16}\,x_9x_{11}x_{12}-(4\cdot10^2)_{16}\,x_{10}x_{11}x_{12}+(12\cdot10^2)_{16}\,x_9x_{10}x_{11}x_{12}+$$
$$+(4\cdot10^3)_{16}\,x_{13}x_{14}-(\mathrm{B}\cdot10^3)_{16}\,x_{13}x_{15}-(10^4)_{16}\,x_{13}x_{16}+(6\cdot10^3)_{16}\,x_{14}x_{15}+$$
$$+(2\cdot10^3)_{16}\,x_{14}x_{16}-(\mathrm{F}\cdot10^3)_{16}\,x_{15}x_{16}+(7\cdot10^3)_{16}\,x_{13}-(7\cdot10^3)_{16}\,x_{14}+$$
$$+(3\cdot10^3)_{16}\,x_{15}+(6\cdot10^3)_{16}\,x_{16}-(4\cdot10^3)_{16}\,x_{13}x_{14}x_{15}-(10^3)_{16}\,x_{13}x_{14}x_{16}+$$
$$+(1\mathrm{F}\cdot10^3)_{16}\,x_{13}x_{15}x_{16}+(\mathrm{D}\cdot10^2)_{16}\,x_{14}x_{15}x_{16}-(16\cdot10^3)_{16}\,x_{13}x_{14}x_{15}x_{16}+$$
$$+(4\cdot10^4)_{16}\,x_{17}x_{19}-(3\cdot10^4)_{16}\,x_{17}x_{18}+(7\cdot10^4)_{16}\,x_{18}x_{19}+(4\cdot10^4)_{16}\,x_{18}x_{20}-$$
$$-(\mathrm{C}\cdot10^4)_{16}\,x_{19}x_{20}-(2\cdot10^4)_{16}\,x_{17}-(10^4)_{16}\,x_{18}+(10^4)_{16}\,x_{19}+(6\cdot10^4)_{16}\,x_{20}-$$
$$-(10^4)_{16}\,x_{17}x_{18}x_{19}-(7\cdot10^4)_{16}\,x_{17}x_{18}x_{20}+(\mathrm{B}\cdot10^4)_{16}\,x_{17}x_{19}x_{20}-$$
$$-(3\cdot10^4)_{16}\,x_{18}x_{19}x_{20}-(8\cdot10^4)_{16}\,x_{17}x_{18}x_{19}x_{20}+(3\cdot10^5)_{16}\,x_{21}x_{22}-$$
$$-(10^5)_{16}\,x_{21}x_{23}-(4\cdot10^5)_{16}\,x_{21}x_{24}-(\mathrm{C}\cdot10^5)_{16}\,x_{22}x_{23}-(\mathrm{C}\cdot10^5)_{16}\,x_{22}x_{24}-$$
$$-(11\cdot10^5)_{16}\,x_{23}x_{24}-(10^5)_{16}\,x_{21}+(3\cdot10^5)_{16}\,x_{22}+(6\cdot10^5)_{16}\,x_{23}+$$
$$+(7\cdot10^5)_{16}\,x_{24}+(\mathrm{D}\cdot10^5)_{16}\,x_{21}x_{22}x_{23}+(\mathrm{C}\cdot10^5)_{16}\,x_{21}x_{22}x_{24}+$$
$$+(\mathrm{B}\cdot10^5)_{16}\,x_{21}x_{23}x_{24}+(22\cdot10^5)_{16}\,x_{22}x_{23}x_{24}-(2\cdot10^6)_{16}\,x_{21}x_{22}x_{23}x_{24}+$$
$$+(10^7)_{16}\,x_{25}x_{26}+(17\cdot10^6)_{16}\,x_{25}x_{27}+(\mathrm{C}\cdot10^6)_{16}\,x_{25}x_{28}+(\mathrm{B}\cdot10^6)_{16}\,x_{26}x_{27}+$$
$$+(\mathrm{E}\cdot10^6)_{16}\,x_{26}x_{28}-(10^6)_{16}\,x_{27}x_{28}-(\mathrm{D}\cdot10^6)_{16}\,x_{25}-(\mathrm{A}\cdot10^6)_{16}\,x_{26}-$$
$$-(9\cdot10^6)_{16}\,x_{27}-(2\cdot10^6)_{16}\,x_{28}-(1\mathrm{D}\cdot10^6)_{16}\,x_{25}x_{26}x_{27}-$$
$$-(16\cdot10^6)_{16}\,x_{25}x_{26}x_{28}-(2\cdot10^6)_{16}\,x_{25}x_{27}x_{28}-(7\cdot10^6)_{16}\,x_{26}x_{27}x_{28}+$$
$$+(2\cdot10^7)_{16}\,x_{25}x_{26}x_{27}x_{28}+(8\cdot10^7)_{16}\,x_{29}-(2\cdot10^7)_{16}\,x_{29}x_{31}-$$
$$-(5\cdot10^7)_{16}\,x_{29}x_{32}-(7\cdot10^7)_{16}\,x_{30}x_{31}-(\mathrm{C}\cdot10^7)_{16}\,x_{30}x_{32}-$$
$$-(\mathrm{B}\cdot10^7)_{16}\,x_{31}x_{32}-(7\cdot10^7)_{16}\,x_{29}x_{30}+(4\cdot10^7)_{16}\,x_{30}+(\mathrm{C}\cdot10^7)_{16}\,x_{31}+$$
$$+(\mathrm{E}\cdot10^7)_{16}\,x_{32}+(\mathrm{F}\cdot10^7)_{16}\,x_{29}x_{30}x_{31}+(8\cdot10^7)_{16}\,x_{29}x_{30}x_{32}+$$
$$+(\mathrm{D}\cdot10^7)_{16}\,x_{29}x_{31}x_{32}+(3\cdot10^7)_{16}\,x_{30}x_{31}x_{32}-(6\cdot10^7)_{16}\,x_{29}x_{30}x_{31}x_{32}+$$
$$+(1\mathrm{D}4675\mathrm{E}4)_{16}\left(\mathrm{mod}(10^8)_{16}\right),$$

где $\vec{x}=\left(\vec{x}_1\ \vec{x}_2\ \ldots\ \vec{x}_8\right)$.