УДК 519.7

ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ СИСТЕМ ПОДСТАНОВОК ЧИСЛОВЫМИ ПОЛИНОМАМИ

А.К. Вишневский
Краснодарское высшее военное училище (ВИ)
Россия, 350035, Краснодар, Красина, 4
E-mail: vishn.artem@yandex.ru

О.А. Финько
Кубанский государственный технологический университет.
Институт информационных технологий и безопасности.
Россия, 350072, Московская, 2
E-mail: ofinko@yandex.ru

Ключевые слова: система подстановок, числовоя нормальная форма, числовой полином
Key word: system of substitutions, numerical normal form, numerical polynom

Рассмотрены особенности реализации систем подстановок числовыми полиномами (ЧП) на примере систем подстановок шифра ГОСТ 28.147-89. Показано, что верхняя граница сложности реализации ЧП систем подстановок значительно меньше, чем для систем произвольных булевых функций от того же количества переменных.

PARALLEL REALIZATION OF SYSTEMS OF SUBSTITUTIONS BY NUMERICAL POLYNOMS/ A.K. Vishnevsky (Krasnodar higher military school (MI), Russia, 350035, Krasnodar, Krasina street, 4, E-mail: vishn.artem@yandex.ru)./ O.A. Finko (Kuban state technological university. Institute of information technologies and safety. Russia, 350072, Moscow street, 2, E-mail: ofinko@yandex.ru). Features of realisation of systems of substitutions by numerical polynoms (NP) on an example of systems of substitutions of cipher GOST 28.147-89. It is shown, that the top border of complexity of realisation by NP of systems of substitutions is much less than for systems of any boollean functions from the same quantity of variables.

1. Операция подстановки как система булевых функций

Описание числовыми полиномами функций алгебры логики обеспечивает возможность параллельной реализации типовых операций, используемых в симметричных шифрах (Таблица 1) универсальным математическим аппаратом. Это позволяет сократить аппаратные ресурсы и использовать их с макисмальной производительностью [1]:
$\vec{\oplus}$ — векторная операция сложения по $\pmod 2$,
$\lll\ggg$ — циклический сдвиг (влево, вправо) на i разрядов,
$\boxplus$ — сложение по $\pmod{2^n - i}$, $i \in \{0, 1\}$, $n \in N$,
$\boxminus$ — вычитание по $\pmod{2^n - i}$, $i \in \{0, 1\}$, $n \in N$,

Таблица 1. Типовые операции симметричных шифров

	GOST	Kasumi	Blowfish	IDEA	CAST	SAFER	Misty	Camellia	SEAL
$\vec{\oplus}$	$\vec{\oplus}$ (32 bit)	$\vec{\oplus}$ (7,9 bit)	$\vec{\oplus}$ (32 bit)	$\vec{\oplus}$ (16 bit)	$\vec{\oplus}$ (16 bit)	$\vec{\oplus}$ (8 bit)	$\vec{\oplus}$ (7,9 bit)	$\vec{\oplus}$ (64 bit)	$\vec{\oplus}$ (32 bit)
$\lll\ggg$	$11 \lll$	$i \lll$			$i \lll$		$i \lll$	$1 \lll$	$1 \lll$ $\ggg 1$
$\boxplus$	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	
$\otimes$				$2^{16}-1$					

$\|$ — конкатенация,
S — блок подстановки,
P — блок перестановки,
$\otimes$ — умножение по $\pmod{2^n - i}$, $i \in \{0, 1\}$, $n \in N$.

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

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

Таким образом подстановка σ_t степени $k = 2^{\log k}$:

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

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

Система подстановок имеет вид:

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

Тогда вектор булевых значений, принимаемых σ_t ($t \in \{1, 2, \dots, s\}$) (Таблица 2), обозначим как:

$$\vec{\sigma}_t = \left(f_t^{(1)}(\vec{x}_t)\ f_t^{(2)}(\vec{x}_t)\ \dots\ f_t^{(\log k)}(\vec{x}_t) \right), \tag{3}$$

где $f_t^{(i)}(\vec{x}_t)$ — булева функция (БФ), определенная на векторе существенных булевых переменных:

$$\vec{x}_t = \left(x_t^{(1)}\ x_t^{(2)}\ \ldots\ x_t^{(\log k)}\right).$$

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	$\sigma_t^{(1)}$	$f_t^{(1)}(\vec{x}_t^{(1)})$	$f_t^{(2)}(\vec{x}_t^{(1)})$	...	$f_t^{(\log k)}(\vec{x}_t^{(1)})$
2	0	0	...	1	$\sigma_t^{(2)}$	$f_t^{(1)}(\vec{x}_t^{(2)})$	$f_t^{(2)}(\vec{x}_t^{(2)})$	...	$f_t^{(\log k)}(\vec{x}_t^{(2)})$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
k	1	1	...	1	$\sigma_t^{(k)}$	$f_t^{(1)}(\vec{x}_t^{(k)})$	$f_t^{(2)}(\vec{x}_t^{(k)})$	...	$f_t^{(\log k)}(\vec{x}_t^{(k)})$

Соответственно вектор системы (2) подстановок (Таблица 3):

$$\vec{\sigma} = (\vec{\sigma}_1\ \vec{\sigma}_2\ \ldots\ \vec{\sigma}_s),$$

где $\vec{\sigma}$ интерпретируется как система БФ:

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

при этом лексикографический порядок упорядоченных существенных переменных:

$$\vec{x} = \left(x_1^{(1)}\ \ldots\ x_1^{(\log k)}\ \ldots\ x_s^{(1)}\ \ldots\ x_s^{(\log k)}\right),$$

сохраняется для каждой σ_t в отдельности.

Таблица 3. Таблица истинности системы подстановок σ

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

2. Построение числового полинома

Существуют различные способы реализации систем БФ . Определенные приемущества имеет представление в числовой нормальной форме [2].

БФ в ряде случаев могут быть представлены каноническим ЧП и линейными ЧП [1, 3].

ЧП или числовая нормальная форма [4] БФ имеет вид:

$$P(\vec{x}) = \sum_{i=1}^{2^n} a_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \tag{5}$$

где $\vec{x} = (x_1\, x_2\, \dots\, x_n)$, $a_i \in \mathbb{Z}$,

$$(i_1 i_2 \dots i_n)_2 = \sum_{j=1}^{n} 2^{n-j} i_j \; (i_j \in \{0,1\}),$$

$$x_j^{i_j} = \begin{cases} x_j, & i_j = 1, \\ 1, & i_j = 0. \end{cases}$$

Представим $f_t^{(i)}(\vec{x}_t)$ в числовой нормальной форме (5):

$$P^{(i)}(\vec{x}_t) = \sum_{i=1}^{k} a_i x_{t,1}^{i_1} x_{t,2}^{i_2} \dots x_{t,\log k}^{i_{\log k}},$$

где $a_j \in \mathbb{Z}$, $i_j \in \{0,1\}$.

Тогда подсистема БФ (3), соответствующая подстановке σ_t может быть представлена ЧП:

$$\begin{aligned} D_t(\vec{x}_t) &= \sum_{j=1}^{\log k} 2^j P_t^{(j)}(\vec{x}_t) \\ &= \sum_{i=1}^{k} c_i x_{t,1}^{i_1} x_{t,2}^{i_2} \dots x_{t,\log k}^{i_{\log k}}, \end{aligned} \tag{6}$$

где $c_i \in \mathbb{Z}$,

$$(i_1 i_2 \dots i_{\log k})_2 = \sum_{j=1}^{\log k} 2^{\log k - j} i_j \; (i_j \in \{0,1\}),$$

$$x_j^{i_j} = \begin{cases} x_j, & i_j = 1, \\ 1, & i_j = 0. \end{cases}$$

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

$$\begin{aligned} N &= H(\vec{x}) \\ &= \sum_{t=1}^{s} 2^{(t-1)\log k} D_t(\vec{x}_t) \\ &= \sum_{\substack{i=1,\dots,k \\ t=1,\dots,s}} d_{t,i} x_{t,1}^{i_1} x_{t,2}^{i_2} \dots x_{t,\log k}^{i_{\log k}} \pmod{2^{s \log k}}, \end{aligned} \tag{7}$$

где $d_{t,j} \in \mathbb{Z}_{2^{s\log k}}$, $N = (y_1 y_2 \dots y_{s\log k})_2$ — представление числа N в двоичной системе счисления, в котором разряды $y_1, y_2, \dots, y_{s\log k}$ являются результатом вычисления БФ:

$$f_s^{(\log k)}(\vec{x}_s), \dots, f_s^{(1)}(\vec{x}_s), \dots, f_1^{(\log k)}(\vec{x}_1), \dots, f_1^{(1)}(\vec{x}_1).$$

3. Алгоритм построения числового полинома систем БФ

Реализацию БФ ЧП можно свести к строгой последовательности действий, которую в свою очередь можно реализовать аппаратно-программными средствами.

1. Построение таблицы истинности n-местной, d-выходной БФ (Таблица 4).

Таблица 4. Таблица истинности n - местной, d - выходной БФ

№	x_1	x_2	…	x_n	y_1	y_2	…	y_d
1	0	0	…	0	$y_1(00\dots0)$	$y_2(00\dots0)$	…	$y_d(00\dots0)$
2	0	0	…	1	$y_1(00\dots1)$	$y_2(00\dots1)$	…	$y_d(00\dots1)$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
2^n	1	1	…	1	$y_1(11\dots1)$	$y_2(11\dots1)$	…	$y_d(11\dots1)$

2. Вычисление вектора истинности: $\vec{Y} = (Y_1\ Y_2\ \dots\ Y_{2^n})^\top$, где

$$Y_i = \sum_{j=1}^{d} 2^{j-1} y_i^j.$$

3. Вычисление коэфициентов ЧП (6):

$$\vec{c} = \mathbf{A}_{2^n}\vec{Y},$$

где $\vec{c} = [c_0\ c_1\ \dots\ c_{2^n-1}]^\top$ — вектор коэффициентов (6) (арифметический спектр БФ [5]). Матрица

$$\mathbf{A}_{2^n} = \begin{bmatrix} \mathbf{A}_{2^{n-1}} & 0 \\ -\mathbf{A}_{2^{n-1}} & \mathbf{A}_{2^{n-1}} \end{bmatrix}$$

являтся n-ой кронекеровской степенью

$$\mathbf{A}_{2^n} = \bigotimes_{t=1}^{n} \mathbf{A}_1$$

базовой матрицы $\mathbf{A}_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$.

4. Умножение вектора мономов в соответствии с их лексикографическим порядком на вектор-столбец коэффициентов ЧП:

$$P(\vec{x}) = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \dots \\ c_{2^n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x_n \\ x_{n-1} \\ x_{n-1}x_n \\ \dots \\ x_1 x_2 \dots x_n \end{bmatrix}.$$

5. Вычисление j-го выходного значения БФ на i-том наборе переменных [5]:

$$y_i^{(j)} = \left\lfloor \frac{P(\vec{x})}{2^j} \right\rfloor \pmod 2.$$

4. Пример

Реализация блока подстановок шифра ГОСТ 28.147-89. Значения подстановок взяты из [6]:

$$\sigma_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 10 & 9 & 2 & 13 & 8 & 0 & 14 & 6 & 11 & 1 & 12 & 7 & 15 & 5 & 3 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 11 & 4 & 12 & 6 & 13 & 15 & 10 & 2 & 3 & 8 & 1 & 0 & 7 & 5 & 9 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 8 & 1 & 13 & 10 & 3 & 4 & 2 & 14 & 15 & 12 & 7 & 6 & 0 & 9 & 11 \end{pmatrix},$$

$$\sigma_4 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 13 & 10 & 1 & 0 & 8 & 9 & 15 & 14 & 4 & 6 & 12 & 11 & 2 & 5 & 3 \end{pmatrix},$$

$$\sigma_5 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 6 & 12 & 7 & 1 & 5 & 15 & 13 & 8 & 4 & 10 & 9 & 14 & 0 & 3 & 11 & 2 \end{pmatrix},$$

$$\sigma_6 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 11 & 10 & 0 & 7 & 2 & 1 & 13 & 3 & 6 & 8 & 5 & 9 & 12 & 15 & 14 \end{pmatrix},$$

$$\sigma_7 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 11 & 4 & 1 & 3 & 15 & 5 & 9 & 0 & 10 & 14 & 7 & 6 & 8 & 2 & 12 \end{pmatrix},$$

$$\sigma_8 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 15 & 13 & 0 & 5 & 7 & 10 & 4 & 9 & 2 & 3 & 14 & 6 & 11 & 8 & 12 \end{pmatrix}.$$

Вычисление ЧП (6) для каждой подстановки:

$$D_1(\vec{x}_1) = 2x_1 - 10x_1x_3 - x_1x_4 - 18x_2x_3 - 11x_2x_4 - \\ - 13x_3x_4 - 8x_1x_2 + 9x_2 + 5x_3 + 6x_4 + 21x_1x_2x_3 + \\ + 14x_1x_2x_4 + 19x_1x_3x_4 + 32x_2x_3x_4 - 48x_1x_2x_3x_4 + 4,$$

$$D_2(\vec{x}_2) = 6x_5x_6 + 16x_5x_7 + 4x_5x_8 + 19x_6x_7 + 10x_6x_8 + \\ + 11x_7x_8 - 12x_5 - 8x_6 - 10x_7 - 3x_8 - 20x_5x_6x_7 - \\ - 19x_5x_7x_8 - 23x_6x_7x_8 + 28x_5x_6x_7x_8 + 14,$$

$$D_3(\vec{x}_3) = 2x_9x_{11} - 13x_9x_{10} - 2x_9x_{12} - 2x_{10}x_{11} - 10x_{10}x_{12} +$$
$$+ 9x_{11}x_{12} + 9x_9 + 5x_{10} - 4x_{11} + 3x_{12} + 7x_9x_{10}x_{11} + 3x_9x_{10}x_{12} -$$
$$- 15x_9x_{11}x_{12} - 4x_{10}x_{11}x_{12} + 18x_9x_{10}x_{11}x_{12} + 5,$$

$$D_4(\vec{x}_4) = 4x_{13}x_{14} - 11x_{13}x_{15} - 16x_{13}x_{16} + 6x_{14}x_{15} + 2x_{14}x_{16} -$$
$$- 15x_{15}x_{16} + 7x_{13} - 7x_{14} + 3x_{15} + 6x_{16} - 4x_{13}x_{14}x_{15} - x_{13}x_{14}x_{16} +$$
$$+ 31x_{13}x_{15}x_{16} + 13x_{14}x_{15}x_{16} - 22x_{13}x_{14}x_{15}x_{16} + 7,$$

$$D_5(\vec{x}_5) = 4x_{17}x_{19} - 3x_{17}x_{18} + 7x_{18}x_{19} + 4x_{18}x_{20} - 12x_{19}x_{20} - 2x_{17} - x_{18} +$$
$$+ x_{19} + 6x_{20} - x_{17}x_{18}x_{19} - 7x_{17}x_{18}x_{20} + 11x_{17}x_{19}x_{20} -$$
$$- 3x_{18}x_{19}x_{20} - 8x_{17}x_{18}x_{19}x_{20} + 6,$$

$$D_6(\vec{x}_6) = 3x_{21}x_{22} - x_{21}x_{23} - 4x_{21}x_{24} - 12x_{22}x_{23} - 12x_{22}x_{24} -$$
$$- 17x_{23}x_{24} - x_{21} + 3x_{22} + 6x_{23} + 7x_{24} + 13x_{21}x_{22}x_{23} + 12x_{21}x_{22}x_{24} +$$
$$+ 11x_{21}x_{23}x_{24} + 34x_{22}x_{23}x_{24} - 32x_{21}x_{22}x_{23}x_{24} + 4,$$

$$D_7(\vec{x}_7) = 16x_{25}x_{26} + 23x_{25}x_{27} + 12x_{25}x_{28} + 11x_{26}x_{27} + 14x_{26}x_{28} -$$
$$- x_{27}x_{28} - 13x_{25} - 10x_{26} - 9x_{27} - 2x_{28} - 29x_{25}x_{26}x_{27} - 22x_{25}x_{26}x_{28} -$$
$$- 16x_{25}x_{27}x_{28} - 7x_{26}x_{27}x_{28} + 32x_{25}x_{26}x_{27}x_{28} + 13,$$

$$D_8(\vec{x}_8) = 8x_{29} - 18x_{29}x_{31} - 21x_{29}x_{32} - 7x_{30}x_{31} - 12x_{30}x_{32} -$$
$$- 27x_{31}x_{32} - 7x_{29}x_{30} + 4x_{30} + 12x_{31} + 14x_{32} + 15x_{29}x_{30}x_{31} +$$
$$+ 24x_{29}x_{30}x_{32} + 45x_{29}x_{31}x_{32} + 19x_{30}x_{31}x_{32} - 38x_{29}x_{30}x_{31}x_{32} + 1,$$

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

Вычисление общего ЧП (7) для восьми подстановок:

$$
\begin{aligned}
H(\vec{x}) = {} & 2x_1 - 10x_1x_3 - x_1x_4 - 18x_2x_3 - 11x_2x_4 - 13x_3x_4 - 8x_1x_2 + \\
& + 9x_2 + 5x_3 + 6x_4 + 21x_1x_2x_3 + 14x_1x_2x_4 + 19x_1x_3x_4 + \\
& + 32x_2x_3x_4 - 48x_1x_2x_3x_4 + 96x_5x_6 + 256x_5x_7 + 64x_5x_8 + \\
& + 304x_6x_7 + 160x_6x_8 + 176x_7x_8 - 192x_5 - 128x_6 - 160x_7 - \\
& - 48x_8 - 320x_5x_6x_7 - 304x_5x_7x_8 - 368x_6x_7x_8 + \\
& + 448x_5x_6x_7x_8 + 512x_9x_{11} - 3328x_9x_{10} - 512x_9x_{12} - \\
& - 512x_{10}x_{11} - 2560x_{10}x_{12} + 2304x_9 + 1280x_{10} - 1024x_{11} + 2304x_{11}x_{12} + \\
& + 768x_{12} + 1792x_9x_{10}x_{11} + 768x_9x_{10}x_{12} - 3840x_9x_{11}x_{12} - \\
& - 1024x_{10}x_{11}x_{12} + 4608x_9x_{10}x_{11}x_{12} + 16384x_{13}x_{14} - \\
& - 45056x_{13}x_{15} - 65536x_{13}x_{16} + 24576x_{14}x_{15} + 8192x_{14}x_{16} - \\
& - 61440x_{15}x_{16} + 28672x_{13} - 28672x_{14} + 12288x_{15} + \\
& + 24576x_{16} - 16384x_{13}x_{14}x_{15} - 4096x_{13}x_{14}x_{16} + 126976x_{13}x_{15}x_{16} + \\
& + 53248x_{14}x_{15}x_{16} - 90112x_{13}x_{14}x_{15}x_{16} + 262144x_{17}x_{19} - \\
& - 196608x_{17}x_{18} + 458752x_{18}x_{19} + 262144x_{18}x_{20} - 786432x_{19}x_{20} - \\
& - 131072x_{17} - 65536x_{18} + 65536x_{19} + 393216x_{20} - 65536x_{17}x_{18}x_{19} - \\
& - 458752x_{17}x_{18}x_{20} + 720896x_{17}x_{19}x_{20} - 196608x_{18}x_{19}x_{20} - \\
& - 524288x_{17}x_{18}x_{19}x_{20} + 3145728x_{21}x_{22} - 1048576x_{21}x_{23} - \\
& - 4194304x_{21}x_{24} - 12582912x_{22}x_{23} - 12582912x_{22}x_{24} - \\
& - 17825792x_{23}x_{24} - 1048576x_{21} + 3145728x_{22} + 6291456x_{23} + \\
& + 7340032x_{24} + 13631488x_{21}x_{22}x_{23} + 12582912x_{21}x_{22}x_{24} + \\
& + 11534336x_{21}x_{23}x_{24} + 35651584x_{22}x_{23}x_{24} - \\
& - 33554432x_{21}x_{22}x_{23}x_{24} + 268435456x_{25}x_{26} + \\
& + 385875968x_{25}x_{27} + 201326592x_{25}x_{28} + 184549376x_{26}x_{27} + \\
& + 234881024x_{26}x_{28} - 16777216x_{27}x_{28} - 218103808x_{25} - \\
& - 167772160x_{26} - 150994944x_{27} - 33554432x_{28} - \\
& - 486539264x_{25}x_{26}x_{27} - 369098752x_{25}x_{26}x_{28} - \\
& - 268435456x_{25}x_{27}x_{28} - 117440512x_{26}x_{27}x_{28} + \\
& + 536870912x_{25}x_{26}x_{27}x_{28} + 2147483648x_{29} - 4831838208x_{29}x_{31} - \\
& - 5637144576x_{29}x_{32} - 1879048192x_{30}x_{31} - 3221225472x_{30}x_{32} - \\
& - 7247757312x_{31}x_{32} - 1879048192x_{29}x_{30} + 1073741824x_{30} + \\
& + 3221225472x_{31} + 3758096384x_{32} + 4026531840x_{29}x_{30}x_{31} + \\
& + 6442450944x_{29}x_{30}x_{32} + 12079595520x_{29}x_{31}x_{32} + \\
& + 5100273664x_{30}x_{31}x_{32} - 10200547328x_{29}x_{30}x_{31}x_{32} + 491156964.
\end{aligned}
$$

5. Оценка полученного числового полинома

Верхняя граница сложности ЧП L системы подстановок (2) от $s \log k$ переменных равна [7]:

$$L = s(2^{\log k} - 1) + 1,$$

что для ГОСТ 28.147-89 составляет:

$$L = 8(2^4 - 1) + 1 = 121,$$

но в тоже время верхняя граница сложности ЧП L_1 для системы произвольных БФ от того же количества переменных равна:

$$L_1 = 2^{s \log k} = 2^{32} = 4292967296.$$

Т.е. при равных количествах переменных в частном и общем случаях выигрыш в сложности ЧП составляет:

$$\frac{L_1}{L} = \frac{4292967296}{121} \approx 35495597 \text{ раз.}$$

Список литературы

1. Финько О.А., Вишневский А.К. Реализация дискретных криптографических функций линейными числовыми полиномами, 29 Всероссийская ВНТК, г. Серпухов, 2010.
2. Закревский А.Д., Торопов Н.Р. Полиномиальная реализация частичных булевых функций и систем. Изд. 2-е, стереотипное. — М.: Едиториал УРСС, 2003. — 200 с. — 200 с.
3. Криптографические методы защиты информации: Коллективная монография: Гл.: 5-7, Сер.: Защита информации, кн. 4, ред. Е.М. Сухарев, Радиотехника, М., 2007, 312 с.
4. Логачев О.А., Сальников А.А., Ященко В.В., Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
5. Финько О.А. Модулярная арифметика параллельных логических вычислений: Монография/[Под ред. В.Д. Малюгина], Ин-т проблем управления им. В.А. Трапезникова РАН; 2003. — 224 с.: ил. http://www.computer-museam.ru/books/archiv/sokcon26.pdf.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. М.: ТРИУМФ, 2003. — 816 с.
7. Финько О.А., Вишневский А.К., Реализация систем подстановок числовыми полиномами. XVII Всероссийская школа-коллоквиум по стохастическим методам, г. Кисловодск, 2010.