15. *Алферов А.П., Зубов А.Ю.* Основы криптографии: Учеб. пособие. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480 с.
16. *Мостеллер Ф., Рурке Р.* Вероятность. – М.: Мир, 1969. – 435 с.

Самойленко Дмитрий Владимирович
Краснодарское высшее военное училище (ВИ).
E-mail: sam-0019@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79183624109.

Финько Олег Анатольевич
Кубанский государственный технологический университет.
Институт информационных технологий и безопасности.
E-mail: ofinko@yandex.ru.
350072, г. Краснодар, ул. Московская, 2.
Тел.: +79615874848.

Samoylenko Dmitry Vladimirovich
Krasnodar higher military school (MI).
E-mail: sam-0019@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79183624109.

Finko Oleg Anatol'evich
Kuban state technological university.
Institute of information technologies and safety.
E-mail: ofinko@yandex.ru.
2, Moscow, Krasnodar, 350072, Russia.
Phone: +79615874848.

УДК 519.7

А.К. Вишневский, В.А. Шарай

РЕАЛИЗАЦИЯ ОПЕРАЦИИ ПОДСТАНОВКИ ЛИНЕЙНЫМИ ЧИСЛОВЫМИ ПОЛИНОМАМИ

Исследована возможность представления операции подстановки степени $k = 2^{\log k}$ *двумя линейными числовыми полиномами на примере первой подстановки криптоалгоритма ГОСТ 28.147-89.*

Линейный числовой полином; криптоалгоритм; криптография; подстановка; числовая нормальная форма; полином Жегалкина; алгебраическая нормальная форма; булева функция; булева формула.

A.K. Vishnevsky, V.A. Sharai

REALIZATION OF OPERATION OF SUBSTITUTION BY THE LINEAR NUMERICAL POLYNOMS

Possibility of representation by two linear numerical polynoms of operation of substitution of degree $k = 2^{\log k}$ *is investigated on example of the first substitution of crypto algorithm GOST 28.147-89.*

Linear numerical polynom; cryptoalgorithm; cryptography; substitution; a numerical normal form; polynom of Gegalkin, an algebraic normal form; boollean function; boollean formula.

Введение. В аппаратных средствах шифрования асимметрические и симметрические криптографические системы (КС) используются совместно, как гибридная КС [1]. При этом асимметрическая КС выполняет функцию шифрования секретных ключей и обмен ими между абонентами. Симметрическая система обеспечивает основной обмен данными между абонентами.

Асимметрическая КС реализуется на спецпроцессорах большой разрядности (в настоящее время актуально 1000 и более), симметрическая КС реализуется на процессорах разрядностью 32 и 64 [1]. Очевидно, что спецпроцессор, реализующий асимметрическую КС, основную часть времени остается в бездействии, так как не участвует в зашифровании и расшифровании открытого (закрытого) текста.

Метод описания булевых функций (БФ) числовыми полиномами (ЧП) [3] предоставляет возможность описания КС обоих классов единым математическим аппаратом, который может быть реализован одним спецпроцессором большой разрядности и, тем самым, задействовать его ресурсы с максимальной производительностью.

Известно, что произвольные БФ и системы n-переменных могут быть однозначно представлены каноническим ЧП в общем случае длиной 2^n [3]. Однако известен и более сильный результат – произвольные БФ и системы могут быть представлены не более чем двумя линейными ЧП (ЛЧП) [2-6]. В [6] представлен ряд результатов, демонстрирующих возможность реализации типовых криптографических примитивов каноническими ЧП.

Цель статьи – исследовать возможность реализации логических криптографических функций, в частности подстановок, посредством ЛЧП.

Булевы представления операции подстановки. Операция подстановки степени $k = 2^{\log k}$ используется в составе большинства современных криптографических алгоритмов, в частности ГОСТ 28.147-89, Kasumi, Blowfish, CAST-128, SAFER++, Misty-1, Camellia и т.п.

Подстановка – это взаимно однозначное отображение конечного множества в себя. При соответствующей нумерации (или упорядочении) элементов конечного множества, на котором определена подстановка, ее можно свести на некотором подмножестве натуральных чисел [7]:

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

Таким образом, операцию подстановки степени $k = 2^{\log k}$ можно интерпретировать как $\log k$ -выходную БФ от $\log k$ -переменных:

$$f(\vec{x}) = \begin{cases} f_1(\vec{x}), \\ f_2(\vec{x}), \\ \dots\dots\dots \\ f_{\log k}(\vec{x}), \end{cases} \qquad (2)$$

где $\vec{x} = [x_1\ x_2\ \dots x_{\log k}]$, таблица истинности которой будет иметь вид, представленный табл. 1.

Таблица 1

Таблица истинности $\log k$ -выходной БФ от $\log k$ -переменных

№	x_1	x_2	…	$x_{\log k}$	$f_1(\vec{x})$	$f_2(\vec{x})$	…	$f_{\log k}(\vec{x})$
1	0	0	…	0	$f_1^{(1)}(\vec{x})$	$f_2^{(1)}(\vec{x})$	…	$f_{\log k}^{(1)}(\vec{x})$
2	0	0	…	1	$f_1^{(2)}(\vec{x})$	$f_2^{(2)}(\vec{x})$	…	$f_{\log k}^{(2)}(\vec{x})$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
K	1	1	…	1	$f_1^{(k)}(\vec{x})$	$f_2^{(k)}(\vec{x})$	…	$f_{\log k}^{(k)}(\vec{x})$

Алгоритм 1. Построение ЛЧП-1 (общая схема представлена на рис. 1).

Шаг 1.1. Представление БФ (табл. 1) в алгебраической нормальной форме (полином Жегалкина):

$$G(\vec{x}) = \begin{cases} G_1(\vec{x}) = \bigoplus\limits_{i=1}^{k} g_{1,i} \wedge (x_1^{i_1} \wedge x_2^{i_2} \wedge \ldots \wedge x_{\log k}^{i_{\log k}}), \\ G_2(\vec{x}) = \bigoplus\limits_{i=1}^{k} g_{2,i} \wedge (x_1^{i_1} \wedge x_2^{i_2} \wedge \ldots \wedge x_{\log k}^{i_{\log k}}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ G_{\log k}(\vec{x}) = \bigoplus\limits_{i=1}^{k} g_{\log k,i} \wedge (x_1^{i_1} \wedge x_2^{i_2} \wedge \ldots \wedge x_{\log k}^{i_{\log k}}), \end{cases} \quad (3)$$

получаемых с помощью прямого и обратного матричного преобразования:

$$\vec{g} = \mathbf{A}_{2^n} \vec{y},$$
$$\vec{y} = \mathbf{A}_{2^n} \vec{g},$$

где $\vec{g} = [g_1\ g_2\ \ldots g_k]$ – вектор коэффициентов $g_j \in \{0, 1\}$; $\vec{y}$ – вектор значений БФ в соответствии с таблицей истинности; матрица $\mathbf{A}_{2^n} = \begin{bmatrix} \mathbf{A}_{2^{n-1}} & 0 \\ -\mathbf{A}_{2^{n-1}} & \mathbf{A}_{2^{n-1}} \end{bmatrix}$ является n-ой кронекеровской степенью $\mathbf{A}_{2^n} = \bigotimes\limits_{j=1}^{n} \mathbf{A}_1$ базовой матрицы $\mathbf{A}_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$; $x_1^{i_1} \wedge x_2^{i_2} \wedge \ldots \wedge x_{\log k}^{i_{\log k}}$ – попарно различные элементарные конъюнкции, где $i_j \in \{0, 1\}$.

Шаг 1.2. Линеаризация элементарных конъюнкций:

$$\begin{aligned} f_1'(\vec{x}) &= x_1^{i_1^{(1)}} \wedge x_2^{i_2^{(1)}} \ldots \wedge x_{\log k}^{i_{\log k}^{(1)}}, \\ f_2'(\vec{x}) &= x_1^{i_1^{(2)}} \wedge x_2^{i_2^{(2)}} \ldots \wedge x_{\log k}^{i_{\log k}^{(2)}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k'(\vec{x}) &= x_1^{i_1^{(k)}} \wedge x_2^{i_2^{(k)}} \ldots \wedge x_{\log k}^{i_{\log k}^{(k)}} \end{aligned} \quad (4)$$

с помощью формулы [4]

$$L_i(\vec{x}) = 2^{\lambda_i} - \log k + \sum_{j=1}^{\log k} \{i_j + (-1)^{i_1} x_j\},$$

где $\lambda_i = \left\lceil \log \sum_{j=1}^{\log k} x_j \right\rceil$, $\lceil a \rceil$ – наименьшее целое число $\geq a$, $i \in \{1, 2, ..., k\}$, и получение системы ЛЧП:

$$\begin{aligned} L_1(\vec{x}) &= c^{(1,1)} + x_1^{i_1^{(1)}} + x_2^{i_2^{(1)}} + \ldots + x_{\log k}^{i_{\log k}^{(1)}}, \\ L_2(\vec{x}) &= c^{(1,2)} + x_1^{i_1^{(2)}} + x_2^{i_2^{(2)}} + \ldots + x_{\log k}^{i_{\log k}^{(2)}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_k(\vec{x}) &= c^{(1,k)} + x_1^{i_1^{(k)}} + x_2^{i_2^{(k)}} + \ldots + x_{\log k}^{i_{\log k}^{(k)}}, \end{aligned} \quad (5)$$

где $c^{(1,j)} \in Z$.

Шаг 1.3. Построение ЛЧП-1

$$\boxed{P_1(\vec{x}) = \sum_{i=1}^{k} 2^{\lambda_{i-1}} L_i(\vec{x}) = c_0 + \sum_{j=1}^{\log k} c_j x_j,}$$

где $c_0, c_u \in Z$, $\lambda_0 = 0$, обеспечивающего параллельное вычисление значений элементарных конъюнкций (4).

Алгоритм 2. Построение ЛЧП-2 (общая схема представлена на рис. 2).

Шаг 2.1. Переопределение результатов вычисления ЛЧП-1 $P_1(\vec{x})$:

$$f_1'(\vec{x}) = x_1', \;\; f_2'(\vec{x}) = x_2', \;\; ..., \;\; f_k'(\vec{x}) = x_k'.$$

Шаг 2.2. Линеаризация логических формул, образованных системой полиномов Жегалкина (3)

$$f(\vec{x}) = \begin{cases} f_1(\vec{x}) = g_{1,1} x_1' \oplus g_{1,2} x_2' \oplus \ldots \oplus g_{1,k} x_k', \\ f_2(\vec{x}) = g_{2,1} x_1' \oplus g_{2,2} x_2' \oplus \ldots \oplus g_{2,k} x_k', \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_{\log k}(\vec{x}) = g_{\log k,1} x_1' \oplus g_{\log k,2} x_2' \oplus \ldots \oplus g_{\log k,k} x_k' \end{cases}$$

с помощью формулы [4]

$$L_u'(\vec{x}') = \sum_{i=1}^{k} \{i_j + (-1)^{i_1} x_j'\},$$

где $u, j \in \{1, 2, ..., \log k\}$, и построение системы ЛЧП:

$$\begin{aligned} L_1'(\vec{x}') &= c^{(2,1)} + x_1' + x_2' + \ldots + x_k', \\ L_2'(\vec{x}') &= c^{(2,2)} + x_1' + x_2' + \ldots + x_k', \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_{\log k}'(\vec{x}') &= c^{(2,\log k)} + x_1' + x_2' + \ldots + x_k', \end{aligned} \quad (6)$$

где $c^{(2,j)} \in Z$.

Шаг 2.3. Построение ЛЧП-2

$$P_2(\vec{x}') = \sum_{i=1}^{\log k} 2^{\nu_{i-1}} L_i'(\vec{x}') = c_0' + \sum_{j=1}^{k} c_j' x_j',$$

где $\nu_u = \left\lceil \log \sum_{i=1}^{k} x_i' \right\rceil$, $c_0', c_t' \in Z$, $\nu_0 = 0$.

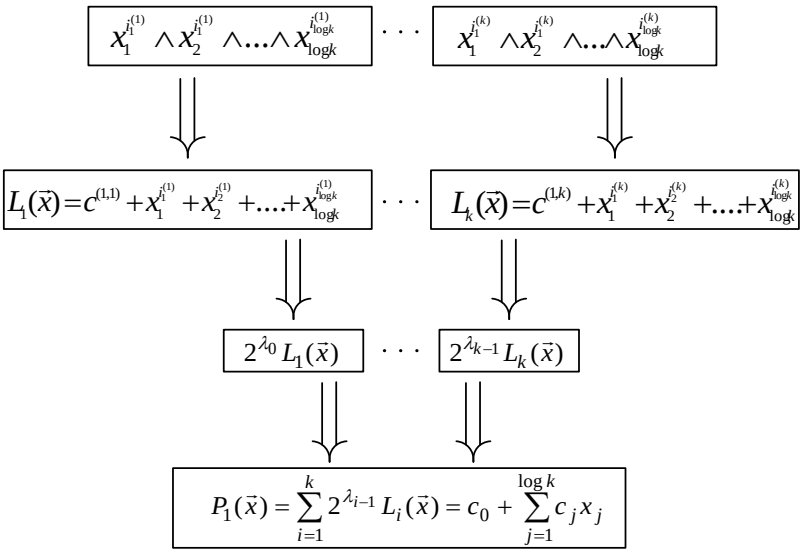

Рис. 1. Схема построения ЛЧП-1 подстановки σ

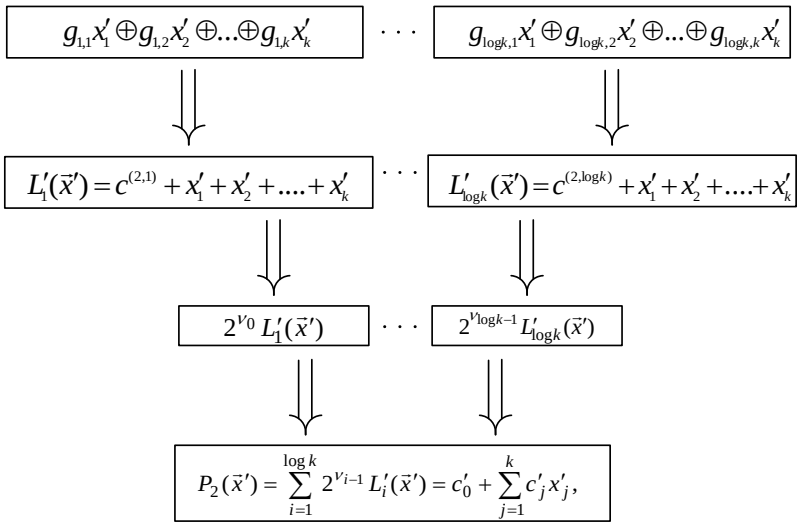

Рис. 2. Схема построения ЛЧП-2 подстановки σ

Алгоритм 3. Реализация ЛЧП-1.

Шаг 3.1. Задание вектора $\vec{x}$ значений входных переменных x_1, x_2, …, $x_{\log k}$ в соответствии с таблицей истинности (табл. 1).

Шаг 3.2. Вычисление ЛЧП-1 $P_1(\vec{x})$ и получение результата, представленного в двоичной системе счисления:

$$P_1(\vec{x}) = \sum_{i=0}^{\lambda_1+\lambda_2+\ldots\lambda_k-1} a_i 2^i = (a_{\lambda_1+\lambda_2+\ldots\lambda_k-1} \ldots a_1\ a_0)_2, \qquad (7)$$

где λ_j – количество двоичных разрядов, необходимых для представления результатов вычисления ЛЧП (5).

Шаг 3.3. Определение значений $y_1, y_2, \ldots y_k$ функций $f_1'(\vec{x})$, $f_2'(\vec{x})$, …, $f_k'(\vec{x})$ с помощью оператора маскирования $\Xi^{\lambda_1+\lambda_2+\ldots+\lambda_j-1}$ [3], предназначенного для вычленения значения $(\lambda_1+\lambda_2+\ldots+\lambda_j-1)$-го двоичного разряда в представлении (7). Например, в представлении $(1\ \ 0\ \ 0\ \ 0)_2$ получим $\Xi^3 = 1$. В общем случае: $\Xi^{\lambda_1+\lambda_2+\ldots+\lambda_j-1} = \left\lfloor \dfrac{P_1(\vec{x})}{2^{\lambda_1+\lambda_2+\ldots+\lambda_i-1}} \right\rfloor \pmod 2 = f_i'(\vec{x})$, где $i \in \{1, 2, ..k\}$.

Алгоритм 4. Реализация ЛЧП-2**.**

Ша 4.1. Переопределение результатов вычисления ЛЧП-1 $P_1(\vec{x})$ $f_1'(\vec{x}) = x_1'$, $f_2'(\vec{x}) = x_2'$, …, $f_k'(\vec{x}) = x_k'$.

Шаг 4.2. Вычисление ЛЧП-2 $P_2(\vec{x}')$ и получение результата, представленного в двоичной системе счисления:

$$P_2(\vec{x}') = \sum_{i=0}^{\nu_1+\nu_2+\ldots\nu_{\log k}-1} b_i 2^i = (b_{\nu_1+\nu_2+\ldots\nu_{\log k}-1} \ldots b_1\ b_0)_2, \qquad (8)$$

где ν_j – количество двоичных разрядов, необходимых для представления результатов вычисления ЛЧП (6).

Шаг 4.3. Определение значений $y_1', y_2', \ldots, y_{\log k}'$ функций $f_1(\vec{x})$, $f_2(\vec{x})$, …, $f_{\log k}(\vec{x})$ с помощью оператора маскирования $\Xi^{\nu_1+\nu_2+\ldots+\nu_{i-1}}$. В общем случае: $\Xi^{\nu_1+\nu_2+\ldots+\nu_{i-1}} = \left\lfloor \dfrac{P_2(\vec{x}')}{2^{\nu_1+\nu_2+\ldots+\nu_{i-1}}} \right\rfloor \pmod 2 = f_i(\vec{x})$, где $i \in \{1, 2, \ldots, \log k\}$, $\nu_0 = 0$.

Блок-схема условно-аппаратной реализации операции произвольной подстановки посредством ЛЧП-1 и ЛЧП-2 представлена на рис. 3.

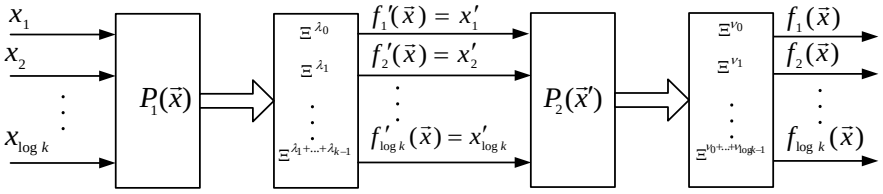

Рис. 3. Блок-схема условно-аппаратной реализации операции произвольной подстановки

Пример. Построение и реализации ЛЧП-1 и ЛЧП-2 первой подстановки криптоалгоритма ГОСТ 28.147-89 (значения подстановки взяты из [8] (табл. 2).

Таблица 2

Значения первой подстановки ГОСТ 28.147-89

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
σ_1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

Результат построения таблицы истинности для подстановки σ_1 в соответствии с табл. 2 представлен в табл. 3.

Таблица 3

Таблица истинности булевого представления подстановки σ_1

№	x_1	x_2	x_3	x_4	№	$f_1(\vec{x})$	$f_2(\vec{x})$	$f_3(\vec{x})$	$f_4(\vec{x})$
1	0	0	0	0	4	0	1	0	0
2	0	0	0	1	10	1	0	1	0
3	0	0	1	0	9	1	0	0	1
4	0	0	1	1	2	0	0	1	0
5	0	1	0	0	13	1	1	0	1
6	0	1	0	1	8	1	0	0	0
7	0	1	1	0	0	0	0	0	0
8	0	1	1	1	14	1	1	1	0
9	1	0	0	0	6	0	1	1	0
10	1	0	0	1	11	1	0	1	1
11	1	0	1	0	1	0	0	0	1
12	1	0	1	1	12	1	1	0	0
13	1	1	0	0	7	0	1	1	1
14	1	1	0	1	15	1	1	1	1
15	1	1	1	0	5	0	1	0	1
16	1	1	1	1	3	0	0	1	1

Построение ЛЧП-1 (для σ_1 ГОСТ 28147-89).

Шаг П.1.1. Представление БФ (табл. 3) в алгебраической нормальной форме:

$$G(\vec{x}) = \begin{cases} G_1(\vec{x}) = x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_4, \\ G_2(\vec{x}) = 1 \oplus x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3, \\ G_3(\vec{x}) = x_4 \oplus x_2x_4 \oplus x_2x_3x_4 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2x_4, \\ G_4(\vec{x}) = x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_3. \end{cases}$$

Шаг П.1.2. Линеаризация элементарных конъюнкций и получение системы ЛЧП (табл. 4).

Шаг П.1.3. Построение ЛЧП-1

$$\begin{aligned} P_1(\vec{x}) = 1 &+ 2x_4 + 2^2x_3 + 2^3(x_3 + x_4) + 2^5x_2 + 2^6(x_2 + x_4) + 2^8(x_2 + x_3 + x_4 + 1) + \\ &+ 2^{11}x_1 + 2^{12}(x_1 + x_4) + 2^{14}(x_1 + x_3) + 2^{16}(x_1 + x_3 + x_4 + 1) + 2^{19}(x_1 + x_2) + \\ &+ 2^{21}(x_1 + x_2 + x_4 + 1) + 2^{24}(x_1 + x_2 + x_3 + 1), \end{aligned}$$

$$\mathrm{P_1(\vec{x}) = 1894016 + 19486720\ x_1 + 19399008\ x_2 + 16859404\ x_3 + 2167114\ x_4.}$$

Таблица 4

Линеаризация элементарных конъюнкций

i	Представление в логической форме	Представление в линейной арифметической форме $L_i(\vec{x})$	λ_i	i	Представление в логической форме	Представление в линейной арифметической форме $L_i(\vec{x})$	λ_i
1	1	1	1	8	x_1	x_1	1
2	x_4	x_4	1	9	x_1x_4	$x_1 + x_4$	2
3	x_3	x_3	1	10	x_1x_3	$x_1 + x_3$	2
4	x_3x_4	$x_3 + x_4$	2	11	$x_1x_3x_4$	$x_1 + x_3 + x_4 + 1$	3
5	x_2	x_2	1	12	x_1x_2	$x_1 + x_2$	2
6	x_2x_4	$x_2 + x_4$	2	13	$x_1x_2x_4$	$x_1 + x_2 + x_4 + 1$	3
7	$x_2x_3x_4$	$x_2 + x_3 + x_4 + 1$	3	14	$x_1x_2x_3$	$x_1 + x_2 + x_3 + 1$	3

Построение ЛЧП-2 (для σ_1 ГОСТ 28147-89).

Шаг П.2.1. Переопределение результатов вычисления ЛЧП-1 $P_1(\vec{x})$

$$f'_1(\vec{x}) = x'_1,\ f'_2(\vec{x}) = x'_2,\ \ldots,\ f'_{14}(\vec{x}) = x'_{14}.$$

Шаг П.2.2. Линеаризация логических выражений, образованных системой полиномов Жегалкина (табл. 5).

Таблица 5

Линеаризация операции XOR

i	Функция	Линейная арифметическая форма $L'_i(\vec{x}')$	ν_i
1	$f_1(\vec{x})$	$x'_2 + x'_3 + x'_5 + x'_6 + x'_7 + x'_{10} + x'_{12} + x'_{13}$	4
2	$f_2(\vec{x})$	$x'_1 + x'_2 + x'_3 + x'_4 + x'_7 + x'_{11} + x'_{13} + x'_{14}$	4
3	$f_3(\vec{x}_1)$	$x'_2 + x'_6 + x'_7 + x'_8 + x'_9 + x'_{10} + x'_{13}$	3
4	$f_4(\vec{x}_1)$	$x'_3 + x'_4 + x'_5 + x'_6 + x'_9 + x'_{11} + x'_{14}$	3

Шаг П.2.3. Построение ЛЧП-2

$$\begin{aligned} P_2(\vec{x}) = {} & x'_2 + x'_3 + x'_5 + x'_6 + x'_7 + x'_{10} + x'_{12} + x'_{13} + \\ & + 2^4(x'_1 + x'_2 + x'_3 + x'_4 + x'_7 + x'_{11} + x'_{13} + x'_{14}) + \\ & + 2^8(x'_2 + x'_6 + x'_7 + x'_8 + x'_9 + x'_{10} + x'_{13}) + \\ & + 2^{11}(x'_3 + x'_4 + x'_5 + x'_6 + x'_9 + x'_{11} + x'_{14}), \end{aligned}$$

$$\boxed{\begin{aligned} P_2(\vec{x}) = {} & 16x'_1 + 273x'_2 + 2605x'_3 + 2064x'_4 + 2049x'_5 + 2305x'_6 + 273x'_7 + 256x'_8 + \\ & + 2304x'_9 + 257x'_{10} + 2064x'_{11} + x'_{12} + 273x'_{13} + 2064x'_{14}. \end{aligned}}$$

Реализация ЛЧП-1 (для σ_1 ГОСТ 28147-89).

Шаг П.3.1. Задание вектора $\vec{x}$ значений входных переменных $x_1 = 1$, $x_2 = 0$, $x_3 = 1$, $x_4 = 0$ из таблицы истинности (см. табл. 3) в ЛЧП-1 $P_1(\vec{x})$

$$\boxed{P_1(\vec{x}) = 1894016 + 19486720 \cdot 1 + 19399008 \cdot 0 + 16859404 \cdot 1 + 2167114 \cdot 0.}$$

Шаг П.3.2. Вычисление ЛЧП-1 $P_1(\vec{x})$, получение результата, представленного в двоичной системе счисления:

$$P_1(\vec{x}) = 55286285 = (01101001011100l101000001101)_2.$$

Шаг П.3.3. Определение значений функций (4) $f_1'(\vec{x})$, $f_2'(\vec{x})$, ..., $f_{14}'(\vec{x})$ с помощью оператора маскирования:

$$\begin{array}{lll}
\Xi^0(P_1(\vec{x})) = f_1'(\vec{x}) = 1, & \Xi^1(P_1(\vec{x})) = f_2'(\vec{x}) = 0, & \Xi^2(P_1(\vec{x})) = f_3'(\vec{x}) = 1, \\
\Xi^4(P_1(\vec{x})) = f_4'(\vec{x}) = 0, & \Xi^5(P_1(\vec{x})) = f_5'(\vec{x}) = 0, & \Xi^7(P_1(\vec{x})) = f_6'(\vec{x}) = 0, \\
\Xi^{10}(P_1(\vec{x})) = f_7'(\vec{x}) = 0, & \Xi^{11}(P_1(\vec{x})) = f_8'(\vec{x}) = 1, & \Xi^{13}(P_1(\vec{x})) = f_9'(\vec{x}) = 0, \\
\Xi^{15}(P_1(\vec{x})) = f_{10}'(\vec{x}) = 1, & \Xi^{18}(P_1(\vec{x})) = f_{11}'(\vec{x}) = 0, & \Xi^{20}(P_1(\vec{x})) = f_{12}'(\vec{x}) = 0, \\
\Xi^{23}(P_1(\vec{x})) = f_{13}'(\vec{x}) = 0, & \Xi^{26}(P_1(\vec{x})) = f_{14}'(\vec{x}) = 0. &
\end{array}$$

Реализация ЛЧП-2 (для σ_1 ГОСТ 28147-89).

Шаг П.4.1. Переопределение результатов вычисления ЛЧП-1 $P_1(\vec{x})$

$$f_1'(\vec{x}) = x_1', \; f_2'(\vec{x}) = x_2', \; \ldots, \; f_{14}'(\vec{x}) = x_{14}',$$

$$\boxed{\begin{array}{l} P_2(\vec{x}) = 16 \cdot 1 + 273 \cdot 0 + 2605 \cdot 1 + 2064 \cdot 0 + 2049 \cdot 0 + 2305 \cdot 0 + 273 \cdot 0 + 256 \cdot 1 + \\ \quad + 2304 \cdot 0 + 257 \cdot 1 + 2064 \cdot 0 + x_{12}' + 273 \cdot 0 + 2064 \cdot 0. \end{array}}$$

Шаг П.4.2. Вычисление ЛЧП-2 $P_2(\vec{x}')$ и получение результата, представленного в двоичной системе счисления:

$$P_2(\vec{x}') = 2594 = (00101000100010)_2.$$

Шаг П.4.3. Определение значений выходных функций:

$$\Xi^0(P_2(\vec{x}')) = f_1(\vec{x}) = 0, \;\; \Xi^4(P_2(\vec{x}')) = f_2(\vec{x}) = 0,$$

$$\Xi^8(P_2(\vec{x}')) = f_3(\vec{x}) = 0, \;\; \Xi^{11}(P_2(\vec{x}')) = f_4(\vec{x}) = 1.$$

Вывод. Таким образом, цель статьи достигнута – доказано, что операцию подстановки можно реализовать не более, чем двумя ЛЧП. Принцип аппаратной реализация рассмотренного метода поясняется с помощью рис. 3.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Алферов А.П., Зубов А.Ю.* Основы криптографии: Учебное пособие. – 2-е изд., испр. и доп. – М., Гелиос АРВ, 2002. – 480 с.
2. *Финько О.А.* Модулярная арифметика параллельных логических вычислений: Монография / Под ред. В.Д. Малюгина. – М.: Ин-т проблем управления им. В.А. Трапезникова РАН; 2003. – 224 с. http://www.computer-museam.ru/books/archiv/sokcon26.pdf.

3. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов. М.: ФИЗМАТЛИТ, 1997. – 192 с.
4. *Yanushkevich S., Shmerko V., Lyshevski S.* Logic design of nanoICs. CRC Press, 2005.
5. *Шалыто А.А.* Логическое управление. Методы аппаратной и программной реализации алгоритмов. – СПб.: Наука, 2000. – 780 с.
6. *Вишневский А.К., Финько О.А.* Реализация некоторых криптографических функций линейными числовыми полиномами // 4-я Международная научно-техническая конференция «Инфокоммуникационные технологии в науке, производстве и образовании». – Ставрополь, 2010. – С. 20-23.
7. *Белоусов А.И., Ткачев С.Б.* Дискретная математика: Учеб. для вузов / Под ред. В.С. Зарубина, А.П. Крищенко. – 3-е изд., стереотип. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 744 с. (Сер. Математика в техническом университете. Вып. XIX).
8. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. – М.: ТРИУМФ, 2003. – 816 с.

Вишневский Артем Константинович
Краснодарское высшее военное училище (ВИ).
E-mail: vishn.artem@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79094603415.

Шарай Вячеслав Александрович
Кубанский государственный технологический университет.
Институт информационных технологий и безопасности.
E-mail: ofinko@yandex.ru.
350072, г. Краснодар, ул. Московская, 2.
Тел.: +79615874848.

Vishnevsky Artem Konstantinovich
Krasnodar higher military school (MI).
E-mail: vishn.artem@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79094603415.

Sharai Viacheslav Aleksandrovich
Kuban state technological university.
Institute of information technologies and safety.
E-mail: ofinko@yandex.ru.
2, Moscow, Krasnodar, 350072, Russia.
Phone: +79615874848.

УДК 004.056:378 (06)

С.Э. Бардаев

МНОГОФАКТОРНАЯ БИОМЕТРИЧЕСКАЯ ПОРОГОВАЯ КРИПТОСИСТЕМА

Предложена биометрическая криптосистема, полученная путем интеграции многофакторной биометрии, пороговой криптографии (схема Шамира) и методов преобразования нечетких биометрических параметров в ключевые последовательности, а также обсуждены преимущества такого решения.

Многофакторная биометрия; пороговые криптографические системы; преобразователь «биометрия – код»; биометрическая криптография; схема Шамира.