УДК 512.624.5 **DOI** 10.15622/sp.59.2

Д.В. САМОЙЛЕНКО, М.А. ЕРЕМЕЕВ, О.А. ФИНЬКО, С.А. ДИЧЕНКО

ПАРАЛЛЕЛЬНЫЙ ЛИНЕЙНЫЙ ГЕНЕРАТОР МНОГОЗНАЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С КОНТРОЛЕМ ОШИБОК ФУНКЦИОНИРОВАНИЯ

Самойленко Д.В., Еремеев М.А., Финько О.А., Диченко С.А. **Параллельный линейный генератор многозначных псевдослучайных последовательностей с контролем ошибок функционирования.**

Аннотация. Предложен параллельный линейный генератор многозначных псевдослучайных последовательностей, функционирующий в условиях генерации аппаратных ошибок, обусловленных деструктивными воздействиями злоумышленника. Рассмотрены основные виды модификации псевдослучайной последовательности при атаках злоумышленника. Отличительной особенностью рассматриваемого итеративного процесса обеспечения достоверности вычислительных операций является «арифметизация» вычислительных операций путем представления системы порождающих рекуррентных логических формул как системы многозначных функций алгебры логики. Последующая реализация многозначных функций алгебры логики посредством арифметических полиномов позволила распараллелить процесс генерации многозначных псевдослучайных последовательностей и нивелировать существующую сложность (специфику) криптографических преобразований логических типов данных, ограничивающих применение методов избыточного кодирования. В результате предложено решение, позволяющее применить избыточные модулярные коды для контроля безошибочности производимых вычислительных операций узлами генерации псевдослучайной последовательности. Причем в отличие от известных решений предлагаемый метод обеспечивает получение фрагментов псевдослучайной последовательности на основании одной рекурсивной арифметической формулы с параллельным контролем ошибок вычислений. Применение модулярных форм позволило перенести вычисления из арифметики поля рациональных чисел в целочисленную арифметику простого поля.

Среди существующего многообразия кодов, исправляющих ошибки (максимально разнесенных кодов), особое место занимают многозначные коды Рида — Соломона. Применение кодов Рида — Соломона при формировании псевдослучайных последовательностей позволяет формировать кодоподобные структуры, осуществляющие контроль и обеспечение достоверности вычислительных операций. Получены расчетные данные вероятности безотказной работы параллельного линейного генератора многозначных псевдослучайных последовательностей с функцией контроля ошибок по принципу функционирования — скользящее резервирование. Достигнутые результаты могут найти широкое применение при реализации перспективных высокопроизводительных средств криптографической защиты информации.

Ключевые слова: *q*-значные псевдослучайные последовательности, линейные рекуррентные регистры сдвига, модулярная арифметика, модулярные формы многозначных функций алгебры логики, средства криптографической защиты информации.

1. Введение.

Для защищенных информационных систем средства криптографической защиты информации (СКЗИ) являются ключевыми и направленны на обеспечение качественных характеристик целевой функции — информирования [1-3].

Особенность реальных условий функционирования СКЗИ характеризуется наличием ряда независимых деструктивных воздействий (атак) злоумышленника, целью которых является снижение безопасности функционирования узлов СКЗИ. При этом среди существующего многообразия известных атак злоумышленника на СКЗИ [4, 5] особым считается вид атак, основанный на инициализации аппаратных ошибок функционирования СКЗИ и направленный на генерацию массовых сбоев их электронных компонентов. Легко заметить, что среди основных компонентов СКЗИ наиболее чувствительными к атакам, основанным на инициализации аппаратных ошибок функционирования, являются генераторы псевдослучайных последовательностей (ПСП) [5]. На рисунке 1 представлена схема основных видов модификации ПСП.

При этом очевидна прямая зависимость безопасного функционирования СКЗИ от узлов формирования ПСП, качества которых во многом определяют свойства СКЗИ в целом.

В настоящее время для обеспечения безошибочности производимых преобразований узлами формирования ПСП разработано множество методов, наиболее распространенными из которых являются структурные методы обнаружения ошибок: поэлементное резервирование, дублирование, избыточная логика и другие, обеспечивающие достаточную обнаруживающую способность, однако при этом требующие больших аппаратурных затрат [6]. Из области цифровой схемотехники известны решения, обеспечивающие безошибочность производимых преобразований над двоичными ПСП, которые основаны на использовании методов избыточного блочного кодирования. Однако в ряде случаев специфика (сложность) криптографических преобразований логических типов данных ограничивает применение данных методов контроля.

В работах [7, 8] предложены решения, преодолевающие сложность применения кодового контроля узлов формирования двоичной ПСП, основанные на «арифметизации» логического счета и применения аппарата кодов системы остаточных классов, обеспечивающие необходимый уровень достоверности их функционирования. Однако особенность полученных решений ограничивается исключительной применимостью при формировании двоичных ПСП. Вместе с тем дальнейшее развитие и проектирование перспективных СКЗИ многие специалисты связывают с применением многозначных функций алгебры логики (МФАЛ) [9, 10]. Применительно к многозначным ПСП, такие решения обусловлены в первую очередь наличием более широкого спектра уникальных свойств по сравнению с двоичной ПСП [10-12]. Вследствие этого возникает необходимость обобщения полученных решений для обеспечения достоверности функционирования узлов формирования многозначных ПСП.

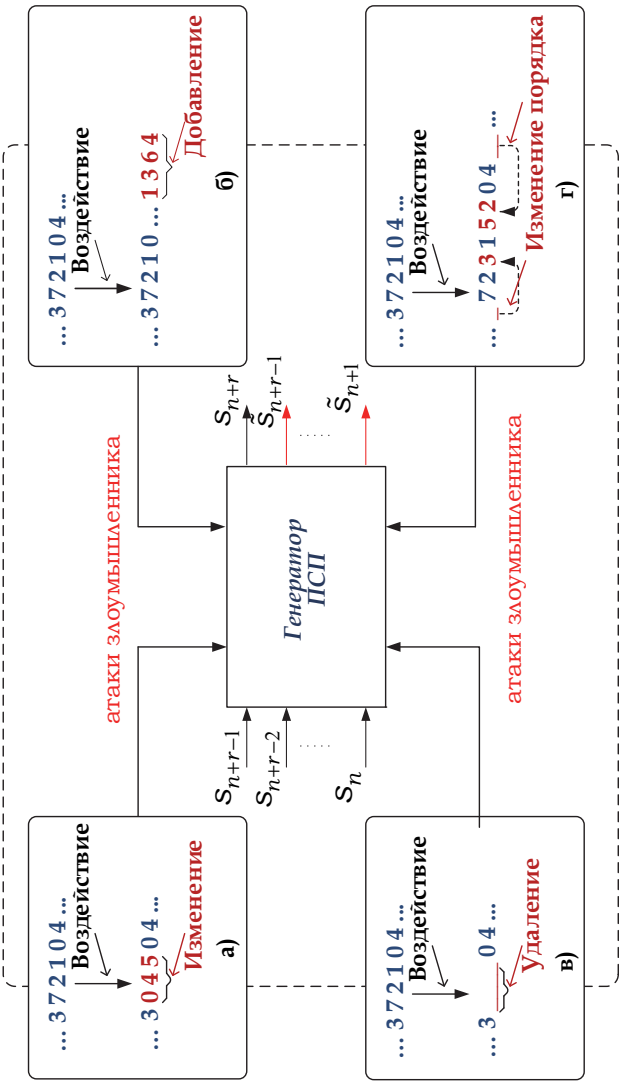

Рис. 1. Схема основных видов модификации ПСП при атаках злоумышленника: а) изменение элементов ПСП; б) добавление новых элементов ПСП; в) удаление элементов ПСП; г) изменение порядка следования элементов ПСП

2. Линейные рекуррентные последовательности над $GF(q)$. Известно, что один из эффективных способов формирования ПСП над $GF(q)$ $(q>2)$ основан на применении переключательных схем специального вида, называемых линейными рекуррентными регистрами сдвига с обратной связью (ЛРРС) [13-15].

В основе синтеза ЛРРС над $GF(q)$ лежит заданный примитивный неприводимый (характеристический) многочлен:

$$P(z)=z^r+p_{r-1}z^{r-1}+p_{r-2}z^{r-2}+\ldots+p_0,$$

где $p_i\in GF(q)$, r — степень полинома $P(z)$, $r\in N$, $GF(q)$ — поле Галуа из q элементов и построенное в соответствии с ним однородное рекуррентное уравнение:

$$s_{n+r}=-p_{r-1}s_{n+r-1}-p_{r-2}s_{n+r-2}-\ldots-p_1s_{n+1}-p_0s_n$$

или:

$$s_{n+r}=p_{r-1}s_{n+r-1}\oplus p_{r-2}s_{n+r-2}\oplus\ldots\oplus p_1s_{n+1}\oplus p_0s_n \pmod q, \qquad (1)$$

где $n=0,1,2,\ldots$; $p_j\in GF(q), 0\le j\le r-1$, $\oplus$ — символ сложения по $(\mathrm{mod}\ q)$.

В общем случае ЛРРС над $GF(q)$ состоит из конструктивных элементов: ячеек D_j $(j=0,1,\ldots,r-1)$, сумматоров по $\mathrm{mod}\ q$, усилителей по $\mathrm{mod}\ q$ и имеет начальное заполнение: $s_0, s_1, \ldots, s_{r-1}$. Под «ячейкой» понимается параллельный $\lceil \log_2 q \rceil$-разрядный регистр ($\lceil x \rceil$ — наименьшее целое число равное или превышающее x). После первого такта работы ЛРРС над $GF(q)$ содержит заполнение $s_1, s_2, \ldots, s_r$. В целом q-ЛРРС генерирует бесконечную q-значную последовательность $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ с периодом q^r-1 (при ненулевом исходном состоянии), причем каждое ненулевое состояние появляется один раз за период. Сформированный сегмент выходной последовательности длины q^r-1 является ПСП над $GF(q)$.

В терминах линейной алгебры очередной q-значный элемент ПСП s_{n+r} вычисляется произведением [8]:

$$\begin{bmatrix} s_{n+r} \\ s_{n+r-1} \\ \dots \\ s_{n+2} \\ s_{n+1} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} s_{n+r-1} \\ s_{n+r-2} \\ \dots \\ s_{n+1} \\ s_n \end{bmatrix}^{\mathrm{T}} \times \begin{bmatrix} p_{r-1} & 1 & 0 & \dots & 0 \\ p_{r-2} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \ddots & \dots \\ p_1 & 0 & 0 & \dots & 1 \\ p_0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

где T — символ транспонирования.

На рисунке 2 представлена обобщенная граф-схема функционирования ЛРРС над $GF(q)$, генерирующего q-значную ПСП.

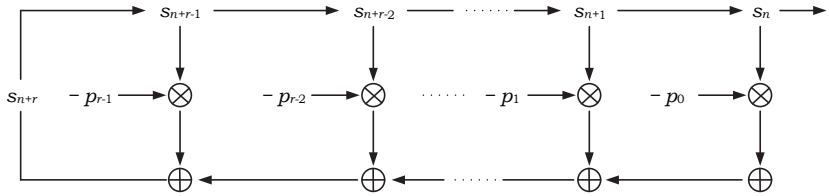

Рис. 2. Граф-схема функционирования ЛРРС над $GF(q)$

3. Многозначные функции алгебры логики. Один из простейших и в тоже время эффективных способов контроля (обнаружения ошибок) в υ-м блоке q-значной ПСП заключается в суммировании элементов υ-го блока ПСП по $\bmod q$ и добавлении в последовательность одного контрольного элемента $\hat{s}_\upsilon$ с тем, чтобы сумма элементов по $\bmod q$ сформированной последовательности соответствовала некоторому эталонному значению ς, например 0. Процедура контроля υ-го блока q-значной ПСП осуществляется в соответствии с выражением:

$$\varsigma_\upsilon^* \equiv \sum_{j=0}^{r-1} s_{\upsilon,j} \oplus \hat{s}_{\upsilon,r} \pmod q, \qquad (2)$$

при этом выполнение условия $\varsigma_\upsilon^* \equiv \varsigma$ свидетельствует об отсутствии обнаруживаемых искажений, в противном случае υ-й блок q-значной ПСП содержит ошибки.

Чтобы обеспечить возможность применения методов кодового контроля к q-значным ПСП, необходимо решить задачу

распараллеливания процесса вычислений q-значной ПСП. При этом в работе [16] в общем виде изложен подход синтеза параллельных генераторов q-значной ПСП на арифметических полиномах, сущность которого заключается в следующем.

Пусть $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ — элементы ПСП, удовлетворяющие многозначному рекуррентному уравнению (1). Ввиду того, что произвольный элемент s_n $(n \geq r)$ последовательности $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ определяется по предшествующим r элементам, представим элементы участка ПСП длиной r $s_{n+r}, s_{n+r+1}, \ldots, s_{n+2r-1}$ в виде системы рекуррентных уравнений:

$$\begin{cases} s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n \pmod q, \\ s_{n+r+1} = p_{r-1}s_{n+r} \oplus p_{r-2}s_{n+r-1} \oplus \ldots \oplus p_0 s_{n+1} \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n+2r-1} = p_{r-1}s_{n+2r-2} \oplus p_{r-2}s_{n+2r-3} \oplus \ldots \oplus p_0 s_{n+r-1} \pmod q, \end{cases} \quad (3)$$

где $\begin{bmatrix} s_{n+r} & s_{n+r+1} & \ldots & s_{n+2r-1} \end{bmatrix}$ — вектор r-того состояния ПСП (или внутреннее состояние q-ЛРРС на r-м такте работы).

По аналогии с [7, 8] выразим правые части системы (3) через заданные начальные условия:

$$\begin{cases} s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n \pmod q, \\ s_{n+r+1} = p_{r-1}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \oplus p_{r-2}s_{n+r-1} \oplus \ldots \\ \qquad \ldots \oplus p_0 s_{n+1} \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n+2r-1} = p_{r-1}(p_{r-1}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \oplus p_{r-2}s_{n+r-1} \oplus \ldots \\ \qquad \ldots \oplus p_0 s_{n+1}) \oplus p_{r-2}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \oplus \ldots \\ \qquad \ldots \oplus p_0(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \pmod q. \end{cases} \quad (4)$$

Упростив выражение (4), запишем полученную систему рекуррентных уравнений как систему r многозначных функций алгебры логики (МФАЛ) от r переменных:

$$\begin{cases} f_1(s_{n+r-1}, \ldots, s_n) = p_{r-1}^{(0)}s_{n+r-1} \oplus p_{r-2}^{(0)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(0)}s_n \pmod q, \\ f_2(s_{n+r-1}, \ldots, s_n) = p_{r-1}^{(1)}s_{n+r-1} \oplus p_{r-2}^{(1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(1)}s_n \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_r(s_{n+r-1}, \ldots, s_n) = p_{r-1}^{(r-1)}s_{n+r-1} \oplus p_{r-2}^{(r-1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(r-1)}s_n \pmod q. \end{cases} \quad (5)$$

Коэффициенты $p_i^{(j)} \in \{0,1,\ldots,q-1\}$ упрощаются (формируются) после сокращения выражения (5). На рисунке 3 представлена схема параллельных вычислений генератора.

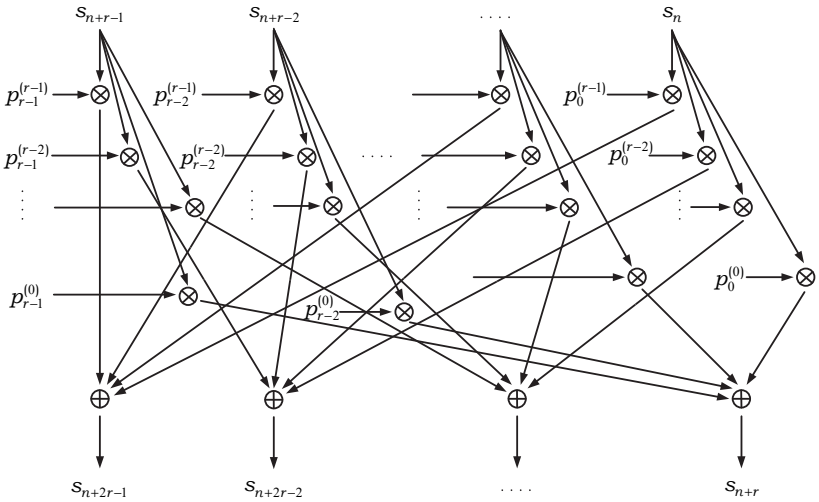

Рис. 3. Граф-схема параллельного q-ЛРРС, функционирующего в соответствии с выражением (5)

Процедура контроля проводимых преобразований (вычислений) для системы (5) МФАЛ может быть обеспечена $(r+1)$ МФАЛ, которая формирует в υ-м блоке q-значной ПСП контрольный элемент.

Тогда система (5) примет вид:

$$\begin{cases} f_1(s_{n+r-1},\ldots,s_n) = p_{r-1}^{(0)} s_{n+r-1} \oplus p_{r-2}^{(0)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(0)} s_n \,(\mathrm{mod}\, q), \\ f_2(s_{n+r-1},\ldots,s_n) = p_{r-1}^{(1)} s_{n+r-1} \oplus p_{r-2}^{(1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(1)} s_n \,(\mathrm{mod}\, q), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_r(s_{n+r-1},\ldots,s_n) = p_{r-1}^{(r-1)} s_{n+r-1} \oplus p_{r-2}^{(r-1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(r-1)} s_n \,(\mathrm{mod}\, q), \\ \hat{f}_{r+1}(s_{n+r-1},\ldots,s_n) = b_{r-1} s_{n+r-1} \oplus b_{r-2} \oplus s_{n+r-2} \oplus \ldots \oplus b_0 s_n \,(\mathrm{mod}\, q), \end{cases} \quad (6)$$

где коэффициенты $\sum_{j=0}^{r-1} p_i^{(j)} \oplus b_i \equiv \varsigma \,(\mathrm{mod}\ q)$ $(\mathrm{i} = 0,1,\ldots,r-1)$.

3.1 Полиномиальная арифметика МФАЛ. В соответствии с [17-20] произвольная МФАЛ может быть представлена в виде арифметического полинома, однозначным образом:

$$A(S) = \sum_{i=0}^{q^{r-1}-1} a_i s_n^{i_0} s_{n+1}^{i_1} \dots s_{n+r-1}^{i_{r-1}} , \tag{7}$$

где a_i — i-й коэффициент арифметического полинома; $S = s_n, s_{n+1}, \dots, s_{n+r-1}$ — аргументы МФАЛ $s_u \in \{0, 1, \dots, q-1\}$ $(u = n, n+1, \dots, n+r-1)$; $(i_0\ i_1 \dots i_{r-1})_q$ — представление параметра i в q-ичной системе счисления:

$$(i_0\ i_1 \dots i_{r-1})_q = \sum_{u=0}^{r-1} i_u q^{r-u-1} \quad (i_u \in \{0, 1, \dots, q-1\});$$

$$s_u^{i_u} = \begin{cases} 1, & i_u = 0, \\ s_u^{i_u}, & i_u \neq 0. \end{cases}$$

Для МФАЛ известен матричный метод построения арифметического полинома [17, 18]. Прямое и обратное матричное преобразование определяется выражениями:

$$\begin{aligned} \mathbf{A} &= N_q^{-1} \mathbf{K}_{q^{r-1}} \mathbf{S}; \\ \mathbf{S} &= \mathbf{K}_{q^{r-1}}^{-1} \mathbf{A}, \end{aligned} \tag{8}$$

где N_k — нормализирующий множитель; $\mathbf{K}_{q^{r-1}}$ и $\mathbf{K}_{q^{r-1}}^{-1}$ — матрицы прямого и инверсного арифметического преобразования размерности $q^{r-1} \times q^{r-1}$ (базис преобразования); $\mathbf{S}$ — вектор истинности МФАЛ:

$$\mathbf{S} = \left[s^{(0)}\ s^{(1)}\ \dots\ s^{(q^{r-1}-1)} \right]^{\mathrm{T}},$$

где $s^{(i)}$ — числовое значение, принимаемое МФАЛ на i-м наборе переменных; вектор коэффициентов арифметического полинома (7):

$$\mathbf{A} = \left[a_0\ a_1\ \dots\ a_{q^{r-1}-1} \right]^{\mathrm{T}}.$$

Матрицы $\mathbf{K}_{q^{r-1}}$ и $\mathbf{K}^{-1}_{q^{r-1}}$ определяются кронекеровским возведением в степень:

$$\mathbf{K}_{q^{r-1}} = \bigotimes_{j=0}^{r-1} \mathbf{K}_q ;$$

$$\mathbf{K}^{-1}_{q^{r-1}} = \bigotimes_{j=0}^{r-1} \mathbf{K}^{-1}_q ,$$

где $\mathbf{K}_q$ и $\mathbf{K}^{-1}_q$ — базовые матрицы прямого и обратного преобразования (таблица 1 – для q = 2, 3, … , 6).

Для МФАЛ $f(S) = 2s_1 \oplus 2s_2 \pmod 3$ вектор принимаемых значений МФАЛ $(r = 2)$ имеет вид: $\mathbf{S} = [0\,1\,2\,2\,1\,0\,1\,0\,2]$. Соответственно, прямое преобразование (8) может быть выражено:

$$\mathbf{A} = \frac{1}{4}\mathbf{K}_{3^2}\mathbf{S} =$$

$$= \frac{1}{4}\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 8 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 0 & 0 & 8 & 0 & 0 & -2 & 0 & 0 \\ 9 & -12 & 3 & -12 & 16 & -4 & 3 & -4 & 1 \\ -3 & 6 & -3 & 4 & -8 & 4 & -1 & 2 & -1 \\ 2 & 0 & 0 & -4 & 0 & 0 & 2 & 0 & 0 \\ -3 & 4 & -1 & 6 & -8 & 2 & -3 & 4 & -1 \\ 1 & -2 & 1 & -2 & 4 & -2 & 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 1 \\ 2 \\ 1 \\ 0 \\ 1 \\ 0 \\ 2 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 0 \\ 14 \\ -6 \\ 14 \\ -24 \\ 6 \\ -6 \\ 6 \\ 0 \end{bmatrix} \begin{matrix} \\ s_2 \\ s_2^2 \\ s_1 \\ s_1 s_2 \\ s_1 s_2^2 \\ s_1^2 \\ s_1^2 s_2 \\ s_1^2 s_2^2 \end{matrix} .$$

Тогда в соответствии с выражением (7) алгебраическая форма примет вид:

$$A(S) = \frac{1}{4}(14s_2 - 6s_2^2 + 14s_1 - 24s_1 s_2 + 6s_1 s_2^2 - 6s_1^2 + 6s_1^2 s_2) .$$

Например, при $s_1 = 2$, $s_2 = 2$ МФАЛ соответствует значение:

$$A(S) = \frac{1}{4}(14\times 2 - 6\times 2^2 + 14\times 2 - 24\times 2\times 2 + 6\times 2\times 2^2 - 6\times 2^2 +$$

$$+6\times 2^2 \times 2) = \frac{1}{4}\times 8 = 2.$$

Таблица 1. Матрицы прямого и обратного преобразования

q	Матрица прямого преобразования, $\mathbf{K}_q$	Матрица обратного преобразования, $\mathbf{K}_q^{-1}$
2	$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
3	$\begin{bmatrix} 2 & 0 & 0 \\ -3 & 4 & -1 \\ 1 & -2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$
4	$\begin{bmatrix} 6 & 0 & 0 & 0 \\ -11 & 18 & -9 & 2 \\ 6 & -15 & 12 & -3 \\ -1 & 3 & -3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \end{bmatrix}$
5	$\begin{bmatrix} 24 & 0 & 0 & 0 & 0 \\ -50 & 96 & -72 & 32 & -6 \\ 35 & -104 & 114 & -56 & 11 \\ -10 & 36 & -48 & 28 & -6 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 6 & 64 & 256 \end{bmatrix}$
6	$\begin{bmatrix} 120 & 0 & 0 & 0 & 0 & 0 \\ -274 & 660 & -660 & 400 & -150 & 24 \\ 225 & -770 & 1070 & -780 & 305 & -20 \\ -85 & 355 & -590 & 490 & -205 & 35 \\ 15 & -70 & 130 & -120 & 55 & -10 \\ -1 & 5 & -10 & 10 & -5 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 \\ 1 & 3 & 9 & 27 & 81 & 243 \\ 1 & 4 & 16 & 64 & 255 & 1024 \\ 1 & 5 & 25 & 125 & 625 & 3125 \end{bmatrix}$

Для трехзначной функции алгебры логики, зависящей от двух переменных, в таблице 2 представлены соответствующие модулярные формы арифметических полиномов.

Таблица 2. Арифметические полиномы для $q = 3, r = 2$

№	Функция	Арифметический полином
1	$s_1 \oplus s_2$	$4^{-1}(4s_2 + 4s_1 + 21s_1s_2 - 15s_1s_2^2 - 15s_2s_1^2 + 9s_1^2s_2^2)$
2	$s_1 \oplus 2s_2$	$4^{-1}(14s_2 - 6s_2^2 + 4s_1 - 39s_1s_2 + 21s_1s_2^2 + 15s_2s_1^2 - 9s_1^2s_2^2)$
3	$2s_1 \oplus s_2$	$4^{-1}(4s_2 + 14s_1 - 39s_1s_2 + 15s_1s_2^2 - 6s_1^2 + 21s_2s_1^2 - 9s_1^2s_2^2)$
4	$2s_1 \oplus 2s_2$	$4^{-1}(14s_2 - 6s_2^2 + 14s_1 - 24s_1s_2 + 6s_1s_2^2 - 6s_1^2 + 6s_1^2s_2)$

В таблице 3 в качестве примера представлены рассчитанные арифметические полиномы для 3-значной функции алгебры логики, зависящей от 3 переменных.

Таблица 3. Арифметические полиномы для $q = 3$, $r = 3$

№	Функция	Арифметический полином
1	$s_1 \oplus s_2 \oplus s_3$	$8^{-1}(8s_3 + 8s_2 + 42s_2s_3 - 30s_2s_3^2 - 30s_3s_2^2 + 18s_2^2s_3^2 + 8s_1 + 42s_1s_3 - 30s_1s_3^2 + +42s_1s_2 - 267s_1s_2s_3 + 135s_1s_2s_3^2 - 30s_1s_2^2 + 135s_1s_2^2s_3 - 63s_1s_2^2s_3^2 - 30s_3s_1^2 + +18s_1^2s_3^2 - 30s_1^2s_2 + 135s_1^2s_2s_3 - 63s_1^2s_2s_3^2 + 18s_1^2s_2^2 - 63s_1^2s_3s_2^2 + 27s_1^2s_2^2s_3^2)$
2	$2s_1 \oplus s_2 \oplus s_3$	$8^{-1}(8s_3 + 8s_2 + 42s_2s_3 - 30s_2s_3^2 - 30s_3s_2^2 + 18s_2^2s_3^2 + 28s_1 - 78s_1s_3 + +30s_1s_3^2 - 78s_1s_2 + 78s_1s_2s_3 + 30s_1s_2^2 - 18s_1s_2^2s_3^2 - 12s_1^2 + 42s_3s_1^2 - -18s_1^2s_3^2 + 42s_1^2s_2 - 72s_1^2s_2s_3 + 18s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 18s_1^2s_3s_2^2)$
3	$s_1 \oplus 2s_2 \oplus s_3$	$8^{-1}(8s_3 + 28s_2 - 78s_2s_3 + 30s_2s_3^2 - 12s_2^2 + 42s_3s_2^2 - 18s_2^2s_3^2 + 8s_1 + 42s_1s_3 - -30s_1s_3^2 - 78s_1s_2 + 78s_1s_2s_3 + 42s_1s_2^2 - 72s_1s_2^2s_3 + 18s_1s_2^2s_3^2 - 30s_3s_1^2 + +18s_1^2s_3^2 + 30s_1^2s_2 - 18s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 18s_1^2s_3s_2^2)$
4	$s_1 \oplus s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 8s_2 - 78s_2s_3 + 42s_2s_3^2 + 30s_3s_2^2 - 18s_2^2s_3^2 + 8s_1 - -78s_1s_3 + 42s_1s_3^2 + 42s_1s_2 + 78s_1s_2s_3 - 72s_1s_2s_3^2 - 30s_1s_2^2 + 18s_1s_2^2s_3^2 + 30s_3s_1^2 - 18s_1^2s_3^2 - 30s_1^2s_2 + 18s_1^2s_2s_3^2 + 18s_1^2s_2^2 - 18s_1^2s_3s_2^2)$
5	$2s_1 \oplus 2s_2 \oplus s_3$	$8^{-1}(8s_3 + 28s_2 - 78s_2s_3 + 30s_2s_3^2 - 12s_2^2 + 42s_3s_2^2 - 18s_2^2s_3^2 + 28s_1 - -78s_1s_3 + 30s_1s_3^2 - 48s_1s_2 + 273s_1s_2s_3 - 135s_1s_2s_3^2 + 12s_1s_2^2 - 117s_1s_3s_2^2 + +63s_1s_2^2s_3^2 - 12s_1^2 + 42s_1^2s_3 - 18s_1^2s_3^2 + 12s_1^2s_2 - 117s_1^2s_2s_3 + 63s_1^2s_2s_3^2 + +45s_1^2s_3s_2^2 - 27s_1^2s_2^2s_3^2)$
6	$2s_1 \oplus s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 8s_2 - 78s_2s_3 + 42s_2s_3^2 + 30s_3s_2^2 - 18s_2^2s_3^2 + 28s_1 - -48s_1s_3 + 12s_1s_3^2 - 78s_1s_2 + 273s_1s_2s_3 - 117s_1s_2s_3^2 + 30s_1s_2^2 - -135s_1s_3s_2^2 + 63s_1s_2^2s_3^2 - 12s_1^2 + 12s_1^2s_3 + 42s_1^2s_2 - 117s_1^2s_2s_3 + +45s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 63s_1^2s_3s_2^2 - 27s_1^2s_2^2s_3^2)$
7	$s_1 \oplus 2s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 28s_2 - 48s_2s_3 + 12s_2s_3^2 - 12s_2^2 + 12s_3s_2^2 + 8s_1 - -78s_1s_3 + 42s_1s_3^2 - 78s_1s_2 + 273s_1s_2s_3 - 117s_1s_2s_3^2 + 42s_1s_2^2 - -117s_1s_3s_2^2 + 45s_1s_2^2s_3^2 + 30s_1^2s_3 - 18s_1^2s_3^2 + 30s_1^2s_2 - 135s_1^2s_2s_3 + +63s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 63s_1^2s_3s_2^2 - 27s_1^2s_2^2s_3^2)$
8	$2s_1 \oplus 2s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 28s_2 - 48s_2s_3 + 12s_2s_3^2 - 12s_2^2 + 12s_3s_2^2 + 28s_1 - -48s_1s_3 + 12s_1s_3^2 - 48s_1s_2 - 57s_1s_2s_3 + 63s_1s_2s_3^2 + 12s_1s_2^2 + 63s_1s_3s_2^2 - -45s_1s_2^2s_3^2 - 12s_1^2 + 12s_1^2s_3 + 12s_1^2s_2 - 63s_1^2s_2s_3 - 45s_1^2s_2s_3^2 - 45s_1^2s_3s_2^2 + +27s_1^2s_2^2s_2^2)$

3.2 Арифметический полином для реализации систем МФАЛ. Реализуем систему МФАЛ (6) посредством вычисления некоторого арифметического полинома. Для этого поставим в соответствие системе МФАЛ (6) систему арифметических полиномов вида (7), один из которых выполняет контроль ошибок вычислений.

Тогда получим:

$$\begin{cases} A_1(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{1,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ A_2(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{2,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_r(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{r,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \hat{A}_{r+1}(S) = \sum\limits_{i=0}^{q^{r-1}-1} a'_{r+1,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}. \end{cases} \quad (9)$$

Умножим полиномы системы (9) на соответствующие веса q^{l-1} $(l = 1,2,\dots,r+1)$:

$$\begin{cases} A_1^*(S) = q^0 A_1(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{1,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ A_2^*(S) = q^1 A_2(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{2,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_r^*(S) = q^{r-1} A_r(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{r,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \hat{A}_{r+1}^*(S) = q^r \hat{A}_{r+1}(S) = \sum\limits_{i=0}^{q^{r-1}-1} \hat{a}_{r+1,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \end{cases}$$

где $a_{l,i}^* = q^{l-1} a_{l,i}$, $a_{r+1,i}^* = q^r a_{r+1,i}$ q^{l-1} $(l = 1,2,\dots,r;\ i = 0,1,\dots,q^{r-1}-1)$.

В результате получим:

$$D(S) = \sum_{i=0}^{q^{r-1}-1} \sum_{l=1}^{r} a^*_{l,\,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1} + \sum_{i=0}^{q^{r-1}-1} \hat{a}^*_{r+1,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}. \qquad (10)$$

Основным недостатком полученного выражения, как правило, считается возможность принятия коэффициентами $a^*_{l,\,i}$, $\hat{a}^*_{r+1,i}$ как положительных, так и отрицательных значений, что требует удваивания числового диапазона по сравнению с использованием неотрицательных коэффициентов. В работе [18] представлены решения представления МФАЛ на основе модулярной формы арифметического полинома, которые осуществляют «перенос» вычислений из поля рациональных чисел $\Re$ в поле $GF(q)$. С использованием модулярных форм МФАЛ [16, 18] выражение (10) примет вид:

$$M(S) = \bigoplus_{i=0}^{q^{r-1}-1} c_i\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1} \pmod{q^r}, \qquad (11)$$

где $c_i = \bigoplus_{l=1}^{r} a^*_{l,\,i} \oplus \hat{a}^*_{r+1,i}$ $(i = 0,1,\dots,q^{r-1}-1)$.

Вычислим значения искомых МФАЛ. Для этого результат вычисления $M(S)$ представим в q-ичной системе счисления и применим оператор маскирования $\Xi^t\{M(S)\}$:

$$\Xi^t\{(s_j^{(1)},\dots,\boxed{s_{j+i}^{(t)}},\dots,s_{j+n}^{(n)})_q\} = \left\lfloor \frac{M(S)}{q^t} \right\rfloor \pmod{q},$$

где t — искомый q-ичный разряд представления $M(S)$. На рисунке 4 представлена схема параллельного генератора с контролем ошибок вычислений, соответствующая выражению (11).

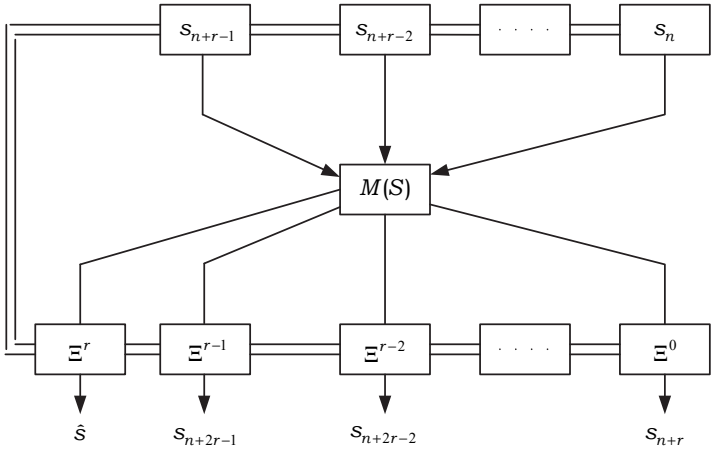

Рис. 4. Схема параллельного q-ЛРРС с контролем ошибок вычислений, функционирующего в соответствии с выражением (11)

Рассмотрим построение 3-ЛРРС, генерирующего 3-значную ПСП, задаваемую характеристическим уравнением: $s_{k+3} = s_{k+2} \oplus 2s_k \pmod 3$ и начальным заполнением: $s_0 = 0, \quad s_1 = 0, \quad s_2 = 2.$

Соответствующий характеристический многочлен имеет вид: $P(z) = z^3 + 2z^2 + 1$.

Тогда система характеристических уравнений для участка ПСП длиной три элемента примет вид:

$$\begin{cases} s_3 = s_2 \oplus 2s_0 \pmod 3, \\ s_4 = s_3 \oplus 2s_1 \pmod 3, \\ s_5 = s_4 \oplus 2s_2 \pmod 3. \end{cases}$$

Далее запишем систему характеристических уравнений как систему с правыми частями равенств, выраженными через заданные начальные условия, с вычисленным уравнением, формирующим контрольный элемент:

$$\begin{cases} f_3(s_2, s_1, s_0) = s_2 \oplus \quad \oplus 2s_0 \pmod 3, \\ f_4(s_2, s_1, s_0) = s_2 \oplus 2s_1 \oplus \quad \oplus 2s_0 \pmod 3, \\ f_5(s_2, s_1, s_0) = \quad 2s_1 \oplus \quad \oplus 2s_0 \pmod 3, \\ \hat{f}(s_2, s_1, s_0) = s_2 \oplus 2s_1 \oplus \quad 0 \pmod 3. \end{cases}$$

В соответствии с (7) получим систему арифметических полиномов следующего вида:

$$\begin{cases} A_3(S) = \frac{1}{4}(4s_2 + 14s_0 - 39s_0s_2 + 15s_0s_2^2 - 6s_0^2 + 21s_2s_0^2 - 9s_0^2s_2^2), \\ A_4(S) = \frac{1}{8}(8s_2 + 28s_1 - 78s_1s_2 + 30s_1s_2^2 - 12s_1^2 + 42s_2s_1^2 - 18s_1^2s_2^2 + 28s_0 - \\ \quad - 78s_0s_2 + 30s_0s_2^2 - 48s_0s_1 + 273s_0s_1s_2 - 135s_0s_1s_2^2 + 12s_0s_1^2 - \\ \quad - 117s_0s_2s_1^2 + 63s_0s_1^2s_2^2 - 12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 12s_0^2s_1 - \\ \quad - 117s_0^2s_1s_2 + 63s_0^2s_1s_2^2 + 45s_0^2s_2s_1^2 - 27s_0^2s_1^2s_2^2), \\ A_5(S) = \frac{1}{4}(14s_1 - 6s_1^2 + 14s_0 - 24s_0s_1 + 6s_0s_1^2 - 6s_0^2 + 6s_0^2s_1), \\ \hat{A}(S) = \frac{1}{4}(4s_2 + 14s_1 - 39s_1s_2 + 15s_1s_2^2 - 6s_1^2 + 21s_2s_1^2 - 9s_1^2s_2^2). \end{cases}$$

Далее систему арифметических выражений реализуем в виде арифметического полинома:

$$\begin{aligned} D(S) &= \frac{1}{4}(4s_2 + 14s_0 - 39s_0s_2 + 15s_0s_2^2 - 6s_0^2 + 21s_2s_0^2 - 9s_0^2s_2^2) + \\ &+ 3^1(\frac{1}{8}(8s_2 + 28s_1 - 78s_1s_2 + 30s_1s_2^2 - 12s_1^2 + 42s_2s_1^2 - 18s_1^2s_2^2 + 28s_0 - \\ &- 78s_0s_2 + 30s_0s_2^2 - 48s_0s_1 + 273s_0s_1s_2 - 135s_0s_1s_2^2 + 12s_0s_1^2 - 117s_0s_2s_1^2 + \\ &+ 63s_0s_1^2s_2^2 - 12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 12s_0^2s_1 - 117s_0^2s_1s_2 + 63s_0^2s_1s_2^2 + \\ &+ 45s_0^2s_2s_1^2 - 27s_0^2s_1^2s_2^2)) + 3^2(\frac{1}{4}(14s_1 - 6s_1^2 + 14s_0 - 24s_0s_1 + 6s_0s_1^2 - 6s_0^2 + \\ &+ 6s_0^2s_1)) + 3^3(\frac{1}{4}(4s_2 + 14s_1 - 39s_1s_2 + 15s_1s_2^2 - 6s_1^2 + 21s_2s_1^2 - 9s_1^2s_2^2)). \end{aligned}$$

Модулярная полиномиальная форма примет вид:

$$\begin{aligned} M(S) &= 5s_0 + 21s_0^2 + 15s_1 + 9s_0s_1 + 18s_0^2s_1 + 63s_1^2 + 18s_0s_1^2 + 31s_2 + 42s_0s_2 + \\ &+ 21s_0^2s_2 + 72s_1s_2 + 72s_0s_1s_2 + 27s_0^2s_1s_2 + 36s_1^2s_2 + 27s_0s_1^2s_2 + \\ &+ 27s_0^2s_1^2s_2 + 15s_0s_2^2 + 72s_0^2s_2^2 + 72s_1s_2^2 + 54s_0^2s_1s_2^2 + \\ &+ 54s_1^2s_2^2 + 54s_0s_1^2s_2^2 \pmod{81}. \end{aligned}$$

В соответствии с заданным начальным заполнением можно получить следующие фрагменты 3-значной ПСП с 1 контрольной цифрой:

$$\textit{шаг } 1 \begin{cases} s_3^{(1)} = \Xi^0\{62\} = \Xi^0\{(2,\ 0,\ 2,\ \boxed{2})_3\} = 2, \\ s_4^{(2)} = \Xi^1\{62\} = \Xi^1\{(2,\ 0,\ \boxed{2},\ 2)_3\} = 2, \\ s_5^{(3)} = \Xi^2\{62\} = \Xi^2\{(2,\ \boxed{0},\ 2,\ 2)_3\} = 0, \\ \hat{s} = \Xi^3\{62\} = \Xi^3\{(\boxed{2},\ 0,\ 2,\ 2)_3\} = 2; \end{cases}$$

$$\textit{шаг } 2 \begin{cases} s_6^{(1)} = \Xi^0\{52\} = \Xi^0\{(1,\ 2,\ 2,\ \boxed{1})_3\} = 1, \\ s_7^{(2)} = \Xi^1\{52\} = \Xi^1\{(1,\ 2,\ \boxed{2},\ 1)_3\} = 2, \\ s_8^{(3)} = \Xi^2\{52\} = \Xi^2\{(1,\ \boxed{2},\ 2,\ 1)_3\} = 2, \\ \hat{s} = \Xi^3\{52\} = \Xi^3\{(\boxed{1},\ 2,\ 2,\ 1)_3\} = 1; \end{cases}$$

$$\textit{шаг } 3 \begin{cases} s_9^{(1)} = \Xi^0\{7\} = \Xi^0\{(0,\ 0,\ 2,\ \boxed{1})_3\} = 1, \\ s_{10}^{(2)} = \Xi^1\{7\} = \Xi^1\{(0,\ 0,\ \boxed{2},\ 1)_3\} = 2, \\ s_{11}^{(3)} = \Xi^2\{7\} = \Xi^2\{(0,\ \boxed{0},\ 2,\ 1)_3\} = 0, \\ \hat{s} = \Xi^3\{7\} = \Xi^3\{(\boxed{0},\ 0,\ 2,\ 1)_3\} = 0; \end{cases}$$

$$\textit{шаг } 4 \begin{cases} s_{12}^{(1)} = \Xi^0\{29\} = \Xi^0\{(1,\ 0,\ 0,\ \boxed{2})_3\} = 2, \\ s_{13}^{(2)} = \Xi^1\{29\} = \Xi^1\{(1,\ 0,\ \boxed{0},\ 2)_3\} = 0, \\ s_{14}^{(3)} = \Xi^2\{29\} = \Xi^2\{(1,\ \boxed{0},\ 0,\ 2)_3\} = 0, \\ \hat{s} = \Xi^3\{29\} = \Xi^3\{(\boxed{1},\ 0,\ 0,\ 2)_3\} = 1; \end{cases}$$

$$\textit{шаг } 5 \begin{cases} s_{15}^{(1)} = \Xi^0\{13\} = \Xi^0\{(0,\ 1,\ 1,\ \boxed{1})_3\} = 1, \\ s_{16}^{(2)} = \Xi^1\{13\} = \Xi^1\{(0,\ 1,\ \boxed{1},\ 1)_3\} = 1, \\ s_{17}^{(3)} = \Xi^2\{13\} = \Xi^2\{(0,\ \boxed{1},\ 1,\ 1)_3\} = 1, \\ \hat{s} = \Xi^3\{13\} = \Xi^3\{(\boxed{0},\ 1,\ 1,\ 1)_3\} = 0; \end{cases}$$

$$\textit{шаг } 6 \begin{cases} s_{18}^{(1)} = \Xi^0\{15\} = \Xi^0\{(0,\ 1,\ 2,\ \boxed{0})_3\} = 0, \\ s_{19}^{(2)} = \Xi^1\{15\} = \Xi^1\{(0,\ 1,\ \boxed{2},\ 0)_3\} = 2, \\ s_{20}^{(3)} = \Xi^2\{15\} = \Xi^2\{(0,\ \boxed{1},\ 2,\ 0)_3\} = 1, \\ \hat{s} = \Xi^3\{15\} = \Xi^3\{(\boxed{0},\ 1,\ 2,\ 0)_3\} = 0; \end{cases}$$

$$\textit{шаг } 7 \begin{cases} s_{21}^{(1)} = \Xi^0\{70\} = \Xi^0\{(2,\,1,\,2,\,\boxed{1})_3\} = 1, \\ s_{22}^{(2)} = \Xi^1\{70\} = \Xi^1\{(2,\,1,\,\boxed{2},\,1)_3\} = 2, \\ s_{23}^{(3)} = \Xi^2\{70\} = \Xi^2\{(2,\,\boxed{1},\,2,\,1)_3\} = 1, \\ \hat{s} = \Xi^3\{70\} = \Xi^3\{(\boxed{2},\,1,\,2,\,1)_3\} = 2; \end{cases}$$

$$\textit{шаг } 8 \begin{cases} s_{24}^{(1)} = \Xi^0\{57\} = \Xi^0\{(2,\,0,\,1,\,\boxed{0})_3\} = 0, \\ s_{25}^{(2)} = \Xi^1\{57\} = \Xi^1\{(2,\,0,\,\boxed{1},\,0)_3\} = 1, \\ s_{26}^{(3)} = \Xi^2\{57\} = \Xi^2\{(2,\,\boxed{0},\,1,\,0)_3\} = 0, \\ \hat{s} = \Xi^3\{57\} = \Xi^3\{(\boxed{2},\,0,\,1,\,0)_3\} = 2; \end{cases}$$

.....

Рассмотрим 3-й блок 3-значной ПСП $[1,2,0,0]$, который не содержит ошибок. В соответствии с выражением (2) вычислим эталонное значение ς_3^*:

$$\varsigma_3^* = \left|1+2+0+0\right|_3 = \left|3\right|_3 = 0\,.$$

Пусть в 8-м блоке 3 ПСП произошла ошибка $\{+2\}$ во втором разряде $\left[0,\tilde{0},0,2\right]$. Тогда $\varsigma_8^* = \left|0+\tilde{0}+0+2\right|_3 = \left|2\right|_3 = 2$.

Полученное эталонное значение $\varsigma_8^* = 2$ не соответствует заданному значению, следовательно, 8-й блок 3 ПСП содержит ошибку.

Положениями [17] вычислительные затраты процесса представления МФАЛ с помощью арифметических полиномов по критерию вычислительной сложности количества операций сложения и умножения при синтезе полиномов и вычислении их значений предполагают: количество операций сложения $(q^{r-1}-1)q^{r-1}$; количество операций умножения — $(q^{r-1})^2$.

4. Контроль ошибок функционирования *q*-ЛРРС многозначными кодами Рида — Соломона. Известно, что среди существующего многообразия «мощных» помехоустойчивых кодов (циклических эквидистантных, Рида — Малера, Боуза — Чоудхури — Хоквингема (БЧХ)) наибольшее распространение

получили коды Рида — Соломона (недвоичные коды БЧХ) [21]. Во-первых, потому что имеют максимально допустимое минимальное кодовое расстояние $d_{\min}$, и следовательно, обладают наибольшей корректирующей способностью, а во-вторых, могут быть систематическими. Как правило, коды Рида — Соломона (РС) задаются с помощью порождающих многочленов $g(z)$, обозначаются как $(m, r, d_{\min})$, где m — длина кодовой комбинации, r — количество информационных символов. При этом несистематический вид кода РС образуется путем произведения порождающего $g(z)$ и информационного многочленов $b(z)$. Систематический — путем сдвига информационного многочлена $b(z)$ на k разрядов, его деление на порождающий многочлен $g(z)$ и добавление полученного остатка $h(z)$ к сдвинутому информационному многочлену $b(z)$. Вместе с тем не менее интересным является решение синтеза кодов РС, основанное на классических преобразованиях в линейных пространствах — матрицах Вандермонда.

4.1 Систематический код РС, основанный на матрицах Вандермонда. Матрица Вандермонда $\mathbf{B}$, состоящая из r строк и m столбцов, определяется последовательностью $[b_0, b_1, \ldots, b_{m-1}]$ элементов, при этом каждый b_i удовлетворяет условию $b_i \in GF(q)$, то есть:

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ b_0 & b_1 & b_2 & \ldots & b_{m-1} \\ b_0^2 & b_1^2 & b_2^2 & \ldots & b_{m-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_0^{r-1} & b_1^{r-1} & b_2^{r-1} & \ldots & b_{m-1}^{r-1} \end{bmatrix}. \qquad (12)$$

Хорошо известно, что для матриц $\mathbf{B}$ над $GF(q)$ характерной структурной особенностью является наличие внутренних вырожденных квадратных подматриц [21, 22], которые препятствуют без дополнительных преобразований их использованию для синтеза систематических кодов РС.

В [21, 22] предложены решения, позволяющие строить порождающие (генераторные) матрицы $\mathbf{G}$ систематической формы на

основе матриц $\mathbf{B}$ для последующего синтеза кодов РС. На первом шаге порождающая матрица $\mathbf{G}$ представляется в виде двух матриц: первой $\mathbf{B}_{r\times r}$, образованной первыми r столбцами второй матрицы $\mathbf{B}_{r\times m}$, определенной ранее. На втором шаге первая матрица $\mathbf{B}_{r\times r}$ инвертируется и умножается на матрицу $\mathbf{B}_{r\times m}$. При этом произведение матриц $\mathbf{B}_{r\times r}^{-1}$ и $\mathbf{B}_{r\times m}$ образует результирующую матрицу $\mathbf{G}$, состоящую в итоге из двух блоков: единичной матрицы $\mathbf{E}_r$ порядка r и следующей за ней матрицы размера $r\times(m-r)$. В общем виде процедуре построения порождающей матрице $\mathbf{G}$ систематической формы соответствует совокупность выражений:

$$\mathbf{G}=\mathbf{B}_{r\times r}^{-1}\times\mathbf{B}_{r\times m}=\left[\mathbf{E}_r\,|\,\mathbf{B}_{r\times r}^{-1}\times\mathbf{B}_{r\times m}\right]=\left[\mathbf{E}_r\,|\,\mathbf{V}_{r\times(m-r)}\right]. \qquad (13)$$

4.2 Кодирование и декодирование ПСП кодами РС. Теперь представим систему характеристических уравнений (4) в виде матричного уравнения:

$$\begin{bmatrix} s_{n+r} \\ s_{n+r+1} \\ \vdots \\ s_{n+2r-1} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} p_{r-1}^{(0)} & p_{r-2}^{(0)} & \cdots & p_0^{(0)} \\ p_{r-1}^{(1)} & p_{r-2}^{(1)} & \cdots & p_0^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ p_{r-1}^{(r-1)} & p_{r-2}^{(r-1)} & \cdots & p_0^{(r-1)} \end{bmatrix} \times \begin{bmatrix} s_{n+r-1} \\ s_{n+r-2} \\ \vdots \\ s_n \end{bmatrix}^{\mathrm{T}},$$

где $\mathbf{P}_r=\left[p_r^{(r)}\right]$ — матрица порядка r.

Далее, заменив в порождающей матрице $\mathbf{G}$ единичную матрицу $\mathbf{E}_r$ на матрицу $\mathbf{P}_r^{\mathrm{T}}$, получим:

$$\mathbf{G}''=\left[\mathbf{P}_r^{\mathrm{T}}\,|\,\mathbf{V}_{r\times(m-r)}\right], \qquad (14)$$

то есть итоговое выражение, позволяющее формировать фрагменты q-значной ПСП длины r с контролем вычислительных операций, которые отождествляются как кодоподобные комбинации кода РС.

Основываясь на классических положениях теории помехоустойчивого кодирования, вполне очевидно, что на полученные кодоподобные q-значные ПСП длины m с r информационными

элементами и $(m-r)$ контрольными элементами соответственно, также распространяются корректирующие свойства кода РС, характеризующиеся числом гарантированно обнаруживаемых

$$\chi_{\text{обн}} \le d_{\min} - 1,$$

и гарантированно исправляемых ошибок

$$\chi_{\text{исп}} \le \left\lfloor \frac{(d_{\min} - 1)}{2} \right\rfloor,$$

в метрике Хэмминга, где $d_{\min} = m - r + 1$, $\lfloor \bullet \rfloor$ — процедура округления до ближайшего меньшего целого числа.

При этом получение υ-го фрагмента q-значной ПСП длины r с контрольными $(m-r)$ цифрами (кодоподобный блок кода РС)

$$\mathbf{S}_\upsilon = \left[s_{\upsilon,\, r-1}\ s_{\upsilon,\, r-2}\ \cdots\ s_{\upsilon,\, 1}\ s_{\upsilon,\, 0}\ \hat{s}_{\upsilon,\, m-r-1}\ \hat{s}_{\upsilon,\, m-r-2}\ \cdots\ \hat{s}_{\upsilon,\, 1}\ \hat{s}_{\upsilon,\, 0} \right]^{\mathrm{T}}$$

находится как скалярное произведение:

$$\mathbf{S}_\upsilon = \mathbf{S}_{\upsilon-1}\mathbf{G}'', \tag{15}$$

где

$$\mathbf{S}_{\upsilon-1} = \left[s_{\upsilon-1,\, r-1}\, s_{\upsilon-1,\, r-2} \cdots s_{\upsilon-1,\, 1}\ s_{\upsilon-1,\, 0}\ \hat{s}_{\upsilon-1,\, m-r-1}\ \hat{s}_{\upsilon-1,\, m-r-2} \cdots \hat{s}_{\upsilon-1,\, 1}\, \hat{s}_{\upsilon-1,\, 0} \right]^{\mathrm{T}}.$$

Известно, что процедура декодирования значительно сложнее процедуры кодирования, вследствие чего проверочной матрице $\mathbf{H}$ необходимо задать специальную форму, при которой последующая процедура декодирования упрощается. Для этого выполним следующие преобразования:

$$\mathbf{H} = (\mathbf{P}_r^{\mathrm{T}})^{-1} \times \mathbf{G}'' = \left[-\mathbf{A}_{r\times(m-r)} \,|\, \mathbf{E}_r \right] = \left[-\mathbf{A}^{\mathrm{T}}_{(m-r)\times r} \,|\, \mathbf{E}_{m-r} \right]. \tag{16}$$

Скалярное произведение υ-го фрагмента q-значной ПСП (кодоподобного блока кода РС) $\mathbf{S}_\upsilon$ на проверочную матрицу $\mathbf{H}$ позволяет получить вектор-синдром $\boldsymbol{\alpha}_\upsilon = \left[\alpha_{\upsilon,\, m-r-1}, \alpha_{\upsilon,\, m-r-2}, \ldots, \alpha_{\upsilon,\, 0} \right]$,

$$\boldsymbol{\alpha}_\upsilon = \mathbf{S}_\upsilon \mathbf{H}^{\mathrm{T}}. \tag{17}$$

Очевидно, что при отсутствии искажений синдром $\boldsymbol{\alpha}_{\upsilon}$ принимает нулевое значение:

$$\boldsymbol{\alpha}_{\upsilon} = 0.$$

Рассмотрим синтез 11-ЛРРС, генерирующего 11-значную ПСП (код РС), задаваемую характеристическим уравнением: $s_{k+7} = 7s_{k+6} \oplus 9s_{k+4} \oplus 9s_{k+1} \oplus 6s_k \pmod{11}$ и начальным заполнением: $s_0 = 1, \quad s_1 = 0, \quad s_2 = 3, \quad s_3 = 0, \quad s_4 = 0, \quad s_5 = 1, \quad s_6 = 7.$

Соответствующий характеристический многочлен имеет вид:

$$P(z) = z^7 + 4z^6 + 2z^4 + 2z + 5.$$

Тогда система характеристических уравнений для участка ПСП длиной семь элементов примет вид:

$$\begin{cases} s_7 = 7s_6 \oplus 9s_4 \oplus 9s_1 \oplus 6s_0 \pmod{11}, \\ s_8 = 7s_7 \oplus 9s_5 \oplus 9s_2 \oplus 6s_1 \pmod{11}, \\ s_9 = 7s_8 \oplus 9s_6 \oplus 9s_3 \oplus 6s_2 \pmod{11}, \\ s_{10} = 7s_9 \oplus 9s_7 \oplus 9s_4 \oplus 6s_3 \pmod{11}, \\ s_{11} = 7s_{10} \oplus 9s_8 \oplus 9s_5 \oplus 6s_4 \pmod{11}, \\ s_{12} = 7s_{11} \oplus 9s_9 \oplus 9s_6 \oplus 6s_5 \pmod{11}, \\ s_{13} = 7s_{12} \oplus 9s_{10} \oplus 9s_7 \oplus 6s_6 \pmod{11}. \end{cases}$$

Далее запишем систему характеристических уравнений как систему с правыми частями равенств, выраженными через заданные начальные условия:

$$\begin{cases} s_7 = 7s_6 \oplus 9s_4 \oplus 9s_1 \oplus 6s_0 \pmod{11}, \\ s_8 = 5s_6 \oplus 9s_5 \oplus 8s_4 \oplus 9s_2 \oplus 3s_1 \oplus 9s_0 \pmod{11}, \\ s_9 = 8s_5 \oplus s_4 \oplus 9s_3 \oplus 3s_2 \oplus 10s_1 \oplus 8s_0 \pmod{11}, \\ s_{10} = 8s_6 \oplus s_5 \oplus 9s_4 \oplus 3s_3 \oplus 10s_2 \oplus 8s_1 \pmod{11}, \\ s_{11} = 2s_6 \oplus 9s_5 \oplus 9s_4 \oplus 10s_3 \oplus 8s_2 \oplus 6s_1 \oplus 4s_0 \pmod{11}, \\ s_{12} = s_6 \oplus 9s_5 \oplus 6s_4 \oplus 8s_3 \oplus 6s_2 \oplus s_0 \pmod{11}, \\ s_{13} = 5s_6 \oplus 6s_5 \oplus 6s_4 \oplus 6s_3 \oplus 10s_2 \oplus 6s_0 \pmod{11}. \end{cases} \quad (18)$$

Построим матрицу $\mathbf{B}$, соответствующую выражению (12):

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \\ 0 & 1 & 8 & 5 & 9 & 4 & 7 & 2 & 6 & 3 & 10 \\ 0 & 1 & 5 & 4 & 3 & 9 & 9 & 3 & 4 & 5 & 1 \\ 0 & 1 & 10 & 1 & 1 & 1 & 10 & 10 & 10 & 1 & 10 \\ 0 & 1 & 9 & 3 & 4 & 5 & 5 & 4 & 3 & 9 & 1 \end{bmatrix},$$

на основании которой, в соответствии с выражением (13), сформируем порождающую матрицу $\mathbf{G}$ (для кода РС) систематической формы:

$$\mathbf{G} = \left[\begin{array}{ccccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 7 & 6 & 7 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 7 & 9 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 10 & 8 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 9 & 7 & 7 & 9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 8 & 10 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 9 & 7 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 7 & 6 & 7 & 1 \end{array}\right]. \quad (19)$$

Представим систему характеристических уравнений (18) в виде матричного уравнения, из которого извлечем матрицу $\mathbf{P}_7$:

$$\mathbf{P}_7 = \begin{bmatrix} 7 & 0 & 9 & 0 & 0 & 9 & 6 \\ 5 & 9 & 8 & 0 & 9 & 3 & 9 \\ 0 & 8 & 1 & 9 & 3 & 10 & 8 \\ 8 & 1 & 9 & 3 & 10 & 8 & 0 \\ 2 & 9 & 9 & 10 & 8 & 6 & 4 \\ 1 & 9 & 6 & 8 & 6 & 0 & 1 \\ 5 & 6 & 6 & 6 & 0 & 10 & 6 \end{bmatrix}.$$

Далее в выражении (19) единичную матрицу $\mathbf{E}_7$ заменим на матрицу $\mathbf{P}_7^{\mathrm{T}}$, в результате получим:

$$\mathbf{G}'' = \left[\begin{array}{ccccccc|cccc} 7 & 5 & 0 & 8 & 2 & 1 & 5 & 1 & 7 & 6 & 7 \\ 0 & 9 & 8 & 1 & 9 & 9 & 6 & 4 & 7 & 9 & 1 \\ 9 & 8 & 1 & 9 & 9 & 6 & 6 & 10 & 8 & 1 & 2 \\ 0 & 0 & 9 & 3 & 10 & 8 & 6 & 9 & 7 & 7 & 9 \\ 0 & 9 & 3 & 10 & 8 & 6 & 0 & 2 & 1 & 8 & 10 \\ 9 & 3 & 10 & 8 & 6 & 0 & 10 & 1 & 9 & 7 & 4 \\ 6 & 9 & 8 & 0 & 4 & 1 & 6 & 7 & 6 & 7 & 1 \end{array}\right].$$

Наконец, фрагменты 11-значной ПСП, формируемые в соответствии с выражением (15) и отождествляемые как систематический код РС с $d_{\min}$=5, имеют вид:

$$\textit{шаг}\ 1\begin{cases} s_{6,7}^{(1)} = 0, \\ s_{5,8}^{(1)} = 3, \\ s_{4,9}^{(1)} = 3, \\ s_{3,10}^{(1)} = 10, \\ s_{2,11}^{(1)} = 7, \\ s_{1,12}^{(1)} = 2, \\ s_{0,13}^{(1)} = 3, \\ \hat{s}_3^{(1)} = 2, \\ \hat{s}_2^{(1)} = 10, \\ \hat{s}_1^{(1)} = 5, \\ \hat{s}_0^{(1)} = 4; \end{cases} \quad \textit{шаг}\ 2\begin{cases} s_{6,14}^{(2)} = 1, \\ s_{5,15}^{(2)} = 4, \\ s_{4,16}^{(2)} = 9, \\ s_{3,17}^{(2)} = 8, \\ s_{2,18}^{(2)} = 9, \\ s_{1,19}^{(2)} = 7, \\ s_{0,20}^{(2)} = 5, \\ \hat{s}_3^{(2)} = 4, \\ \hat{s}_2^{(2)} = 4, \\ \hat{s}_1^{(2)} = 4, \\ \hat{s}_0^{(2)} = 4; \end{cases} \quad \textit{шаг}\ 3\begin{cases} s_{6,21}^{(3)} = 4, \\ s_{5,22}^{(3)} = 9, \\ s_{4,23}^{(3)} = 3, \\ s_{3,24}^{(3)} = 10, \\ s_{2,25}^{(3)} = 4, \\ s_{1,26}^{(3)} = 10, \\ s_{0,27}^{(3)} = 6, \\ \hat{s}_3^{(3)} = 4, \\ \hat{s}_2^{(3)} = 10, \\ \hat{s}_1^{(3)} = 1, \\ \hat{s}_0^{(3)} = 8; \end{cases} \quad \textit{шаг}\ 4\begin{cases} s_{6,28}^{(4)} = 7, \\ s_{5,29}^{(4)} = 0, \\ s_{4,30}^{(4)} = 8, \\ s_{3,31}^{(4)} = 6, \\ s_{2,32}^{(4)} = 2, \\ s_{1,33}^{(4)} = 2, \\ s_{0,34}^{(4)} = 2, \\ \hat{s}_3^{(4)} = 10, \\ \hat{s}_2^{(4)} = 3, \\ \hat{s}_1^{(4)} = 7, \\ \hat{s}_0^{(4)} = 0; \end{cases} \ \ldots,$$

при этом $\chi_{\text{обн}} \le 4$, а $\chi_{\text{исп}} \le 2$.

Далее проверочная матрица **H** систематического кода РС вычисляется по формуле (16) и представляется в следующей форме:

$$\mathbf{H} = \left[\begin{array}{ccccccc|cccc} 6 & 5 & 3 & 3 & 4 & 10 & 10 & 1 & 0 & 0 & 0 \\ 1 & 7 & 8 & 10 & 0 & 9 & 1 & 0 & 1 & 0 & 0 \\ 9 & 2 & 0 & 9 & 2 & 0 & 2 & 0 & 0 & 1 & 0 \\ 10 & 4 & 1 & 9 & 1 & 3 & 7 & 0 & 0 & 0 & 1 \end{array}\right].$$

Рассмотрим 3-й блок 11-значной ПСП $[4, 9, 3, 10, 4, 10, 6, 4, 10, 1, 8]$, не содержащий ошибок. В соответствии с выражением (17) получим вектор-синдром $\boldsymbol{\alpha}_3$:

$$\begin{bmatrix}0\\0\\0\\0\end{bmatrix} = \begin{bmatrix}4\\9\\3\\10\\4\\10\\\underline{6}\\4\\10\\1\\8\end{bmatrix} \times \begin{bmatrix}6&1&9&10\\5&7&2&4\\3&8&0&1\\5&10&9&9\\4&0&2&1\\10&9&0&3\\\underline{10}&\underline{1}&\underline{2}&\underline{7}\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}.$$

Как видно, все четыре компоненты полученного вектора-синдрома равны 0, следовательно, 3-й блок 11-значной ПСП не содержит искажений.

Внесем ошибку. Например, на символы $s^{(4)}_{3,31}$, $s^{(4)}_{0,34}$ воздействует искажение $\{+2\}$, то есть примем за 4-й блок 11-значной ПСП следующее значение $\left[7, 0, 8, \tilde{8}, 2, 2, \tilde{4}, 10, 3, 7, 0\right]$. Найдем вектор-синдром $\boldsymbol{\alpha}_4$:

$$\begin{bmatrix}8\\0\\0\\10\end{bmatrix} = \begin{bmatrix}7\\0\\8\\\underline{8}\\2\\2\\\underline{4}\\10\\3\\7\\0\end{bmatrix} \times \begin{bmatrix}6&1&9&10\\5&7&2&4\\3&8&0&1\\5&10&9&9\\4&0&2&1\\10&9&0&3\\\underline{10}&\underline{1}&\underline{2}&\underline{7}\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}.$$

Полученный вектор-синдром $\boldsymbol{\alpha}_4$ не является нулевым, следовательно, 4-й блок 11-значной ПСП содержит ошибки. При этом

процедура исправления обнаруженных искажений может быть реализована с помощью известных правил [6].

5. Отказоустойчивость функционирования *q*-ЛРРС. Разработанный в настоящей работе подход является, по сути, инструментом решения задачи обеспечения безопасного (надежного) функционирования дискретных устройств. При этом результативность рассматриваемого решения может быть охарактеризована свойством отказоустойчивости. Тогда в качестве показателя отказоустойчивости определим вероятность безотказной работы в течение времени t (показатель $P(t)$). Тогда вероятности безотказной работы $P_{\text{Sl}}(t)$ параллельного многозначного генератора ПСП с функцией контроля ошибок по принципу функционирования — скользящее резервирование соответствует выражение:

$$P_{\text{Sl}}(t) = \sum_{i=0}^{m} \frac{((g-m)\lambda g^{-1}t)^i}{i!} e^{-(g-m)\lambda g^{-1}t},$$

где g — общее число элементов схемы, m — число резервных элементов схемы, λ — интенсивность отказов, $e = 2,71828$ — число Эйлера.

Оценивание произведем, например, при продолжительности эксплуатации 56450 часов и интенсивности отказов – $\lambda = 0,00001$ *час*$^{-1}$. В качестве исходных данных рассмотрим параллельные многозначные генераторы ПСП следующих структур: $g = \{5, 9, 11\}$, $m = 2 - const$. Результаты оценивания приведены в таблице 4.

Таблица 4. Расчетные данные вероятности безотказной работы

Суммарная продолжительность эксплуатации t, час	$P_{\text{Sl1}}(t)$ $g=5,\ m=2$	$P_{\text{Sl2}}(t)$ $g=9,\ m=2$	$P_{\text{Sl3}}(t)$ $g=13,\ m=2$
2400	0.999999	0.999999	0.999999
6050	0.999992	0.999983	0.999978
13250	0.999921	0.999831	0.999784
20450	0.999719	0.999404	0.999241
27650	0.999328	0.998588	0.998207
34850	0.998696	0.997288	0.996569
42050	0.997782	0.995428	0.994237
49250	0.996549	0.992952	0.991146
56450	0.994966	0.989814	0.98725

Графическое представление полученных результатов представлено на рисунке 5.

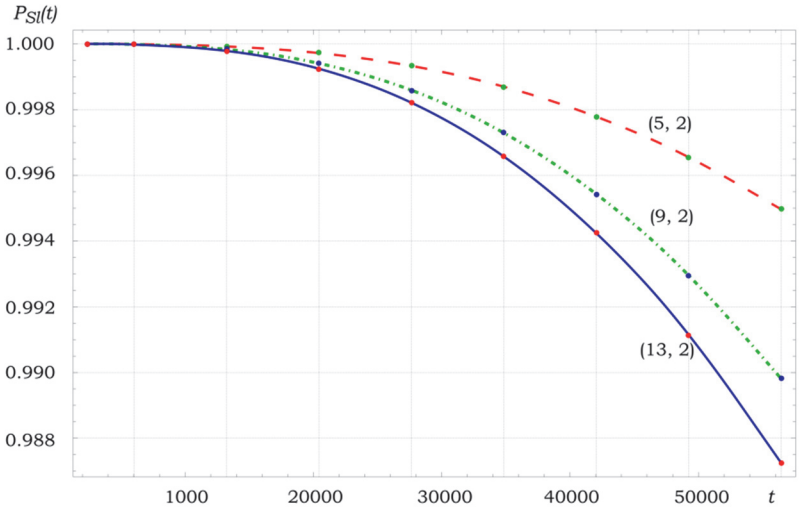

Рис. 5. Зависимость вероятности безотказной работы генератора ПСП от числа информационных элементов g при фиксированном числе контрольных $m - const$

6. Заключение. Представлен параллельный линейный генератор многозначных псевдослучайных последовательностей с контролем ошибок функционирования. Отличительная особенность предлагаемого решения заключается в итеративной процедуре арифметического представления МФАЛ и применения арифметического модулярного кода. Совокупность указанных решений обеспечивает параллельную реализацию фрагментов ПСП с контролем ошибок вычислений в рамках одной рекурсивной арифметической формулы. При этом в реальном масштабе времени обеспечивается функциональный контроль оборудования, что является принципиальным для СКЗИ. Также предложены решения контроля ошибок функционирования многозначных генераторов ПСП, основанные на многозначных помехоустойчивых кодах Рида — Соломона, позволяющие существенно повысить уровень отказоустойчивости без увеличения аппаратной избыточности. И несмотря на то, что в работе рассмотрены классические q-ЛРРС, полученные решения могут лежать в основе синтеза более сложных q-ЛРРС, предназначенных для перспективных высокопроизводительных средств криптографической защиты информации.

Очевидно, что в рамках этой работы не уделяется внимания важной области — оценивания и проверки качества ПСП с контрольными (избыточными) элементами. Однако существующее многообразие различных критериев (тесты автокорреляции, профиля сложности линейной, серий, частот цепочек и т.д.) требует отдельного рассмотрения как направление дальнейших исследований.

Литература

1 *Козлитин О.А.* Использование 2-линейного регистра сдвига для выработки псевдослучайных последовательностей // Математические вопросы криптографии. 2014. № 1. С. 39–72.

2 *Hwang T., Gope P.* Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network // Security and communication networks. 2016. pp. 667–679.

3 *Chen D. et al.* Multi-message Authentication over Noisy Channel with Secure Channel Codes // 2017. arXiv preprint arXiv:1708.02888. 15 p. URL: https://arxiv.org/pdf/1708.02888.pdf (дата обращения: 14.05.2018).

4 *Zou M.H., Ma K, Wu K.J.* Scan-based attack on stream ciphers: A case study on eSTREAM finalists // Computer science and technology. 2014. vol. 29. pp. 646–655.

5 *Yang B., Wu K., Karri R.* Scan Based Side Channel Attack on Data Encryption Standart. IACR Cryptology ePrint Archive. 2004. vol. 2004. 6 p. URL: http://eprint.iacr.org/2004/083.pdf (дата обращения: 14.05.2018).

6 *Хетагуров Я.А., Пруднев Ю.П.* Повышение надежности цифровых устройств методами избыточного кодирования // М.: Энергия. 1974. 270 с.

7 *Диченко С.А., Финько О.А.* Безопасные генераторы псевдослучайных линейных последовательностей на арифметических полиномах для защищенных систем связи // Нелинейный мир. 2013. № 9. С. 632−647.

8 *Finko O.A., Dichenko S.A.* Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms: Soft Computing in Computer and Information Science // Soft computing in computer and information science. 2015. vol. 342. pp. 279−290.

9 *Tao S., Dubrova E.* MVL-PUFs: multiple-valued logic physical unclonable functions // International Journal of Circuit Theory and Applications. 2017. vol. 2. no. 45. pp. 292−304.

10 *Соколов А.В., Жданов О.Н., Айвазян О.А.* Методы синтеза алгебраической нормальной формы функций многозначной логики // Системный анализ и прикладная информатика. 2016. № 1. С. 69–76.

11 *Abd-EI-Barr M., Al-Noori A.* Logic Design and Comparison of Arithmetic Structures for AES Cryptographic Systems // International Conference on Security and Management (SAM'2015). 2015. pp. 185–191.

12 *Abd-EI-Barr M., Al-Noori A.* Arithmetic structures for AES cryptographic systems // 2nd International Conference on Electronics and Communication Systems (ICECS). 2015. pp. 1364–1370.

13 *Gardner D., Sălăgean A., Phan R.C.W.* Efficient Generation of Elementary Sequences: Cryptography and Coding // IMA International Conference on Cryptography and Coding. 2013. LNCS 8308. pp. 16–27.

14 *Kim S-Y., Cho K-R., Lee J-H.* Design of *q*-Parallel LFSR-Based Syndrome Generator // IEICE Transaction on Electronics. 2015. pp. 594–596.

15 *Мельников С.Ю.* Статистические свойства неавтономных обобщенных двоичных регистров сдвига // Доклады Томского государственного университета систем управления и радиоэлектроники. 2017. № 1. С.93−95.

16 *Finko O.A., Samoylenko D.V.* Parallel generator of *q*-valued pseudorandom sequences based on arithmetic polynomials // Przeglad Elektrotechniczny. 2015. vol. 91. no. 3. pp. 24–28.

17 *Антоненко В.М., Иванов А.А., Шмерко В.П.* Линейные арифметические формы *k*-значных логических функций и их реализация на систолических массивах // Автоматика и телемеханика. 1995. № 3. С. 139–155.

18 *Финько О.А.* Модулярные формы систем *k*-значных функций алгебры логики // Автоматика и телемеханика. 2005. № 7. С. 66–86.

19 *Дзюжаньски П., Малюгин В.Д., Шмерко В.П., Янушкевич С.Н.* Линейные модели схем на многозначных элементах // Автоматика и телемеханика. 2002. № 6. С. 99–119.

20 *Мамонтов А.И.* О связи функциональных систем полиномов и арифметических полиномов, представляющих системы булевых функций // Вестник Московского энергетического института. 2017. № 6. С. 161–165.

21 *Mattoussi F., Roca V., Sayadi B.* Complexity Comparison of the Use of Vandermonde versus Hankel Matrices to Build Systematic MDS Reed-Solomon Codes // 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2012. pp. 344–348. URL: https://arxiv.org/pdf/1708.02888.pdf (дата обращения: 14.05.2018).

22 *Mattoussi F., Khalighi A.M, Bourennane S.* Improving the performance of underwater wireless optical communication links by channel coding // Applied Optics. 2018. vol. 57. no. 9. pp. 2115–2120.

Самойленко Дмитрий Владимирович — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: безопасность информации, системы криптокодовой защиты информации, модулярная арифметика многомерных числовых систем. Число научных публикаций — 20. 19sam@mail.ru; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7-812-237-19-60.

Еремеев Михаил Алексеевич — д-р техн. наук, профессор, профессор кафедры прикладных информационных технологий института комплексной безопасности и специального приборостроения, МИРЭА – Российский технологический университет, (РТУ МИРЭА). Область научных интересов: информационная безопасность, криптография, моделирование конфликтующих систем, автоматизированные системы сбора и обработки информации. Число научных публикаций — 200. mae1@rambler.ru; Проспект Вернадского, 78, Москва, 119454; р.т.: +7-812-237-19-60.

Финько Олег Анатольевич — д-р техн. наук, профессор, профессор специальной кафедры, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, академический советник, Российская академия ракетных и артиллерийских наук (отделение технических средств и технологий разведки, навигации, связи и управления). Область научных интересов: параллельные вычисления в системе остаточных классов, числовая реализация систем функций алгебры логики, функциональное диагностирование цифровых устройств избыточными кодами, контроль целостности информации в системах электронного документооборота и других информационных системах, аспекты инженерной реализации криптографических примитивов, системы счисления. Число научных публикаций — 150. ofinko@yandex.ru, http://www.mathnet.ru/rus/person40004; ул. Красина, 4, Краснодар, 350065; р.т.: +79882411171.

Диченко Сергей Александрович — к-т техн. наук, преподаватель, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. Область научных интересов: инженерные аспекты криптографии: компьютерная алгебра, логические вычисления в криптографии, контроль ошибок криптографических преобразований. Число научных публикаций — 30. dichenko.sa@yandex.ru; ул. Красина, 4, Краснодар, 350065; р.т.: 7-861-268-35-09.

DOI 10.15622/sp.59.2

D.V. SAMOYLENKO, M.A. EREMEEV, O.A. FINKO, S.A. DICHENKO

PARALLEL LINEAR GENERATOR OF MULTIVALUED PSEUDORANDOM SEQUENCES WITH OPERATION ERRORS CONTROL

Samoylenko D.V., Eremeev M.A., Finko O.A., Dichenko S.A. **Parallel Linear Generator of Multivalued Pseudorandom Sequences with Operation Errors Control.**

Abstract. A parallel linear generator of multi-valued pseudorandom sequences, which operates under conditions of generating hardware errors caused by destructive adversary actions is proposed. The main types of modification of the pseudorandom sequence in case of adversary attack are considered. A distinctive feature of the iterative process of ensuring the reliability of computational operations is the "arithmetic" of computational operations by representing a system of generating recurring logical formulas as a system of many-valued logic algebra functions. The subsequent realization of multivalued logic algebra functions by means of arithmetic polynomials allowed us to parallelize the process of generating multivalued pseudorandom sequences and level out the existing complexity (specificity) of cryptographic transformations of logical data types which limit the use of redundant coding methods. As a result, a solution that allows to apply redundant modular codes to control the accuracy of the computational operations performed by the nodes of pseudorandom sequence generation is proposed. Moreover, unlike the known solutions, the proposed method provides obtaining fragments of a pseudorandom sequence on the basis of one recursive arithmetic formula with parallel calculation errors control. The use of modular forms made it possible to transfer computations from the rational numbers field arithmetic to integer arithmetic of a simple field.

Among the existing variety of codes correcting errors (maximally spaced codes), a special place is occupied by multivalued Reed-Solomon codes. Reed-Solomon codes usage in the formation of pseudorandom sequences allows the formation of code-like structures that monitor and ensure the reliability of computational operations. The calculated probability of failure-free operation of the parallel linear generator of multivalued pseudorandom sequences with an error control function based on the principle of functioning — sliding redundancy is obtained. The achieved results can find wide application at realization of perspective high-efficiency cryptographic information protection facility.

Keywords: *q*-valued pseudorandom sequences, linear recurrent shift registers, modular arithmetic, modular forms of multivalued, logic algebra functions, cryptographic information protection facility.

Samoylenko Dmitry Vladimirovich — Ph.D., doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, crypto-coded information security systems, and modular arithmetic of multidimensional numerical systems. The number of publications — 20. 19sam@mail.ru; 13, Zhdanovskaya str., St.-Petersburg, 197198, Russia; office phone: +7-812-237-19-60.

Eremeev Mikhail Alekseevich — Ph.D., Dr. Sci., professor, professor of applied information technology the department of institute a comprehensive safety and special instrumentation, MIREA – Russian Technological University. Research interests: information security, cryptography, modeling of the conflicting systems. The number of publications — 200. mae1@rambler.ru; 78, pr. Vernadskogo, Moscow, 119454, Russia; office phone: +7-812-237-19-60.

Finko Oleg Anatolievich — Ph.D., Dr. Sci., professor, professor of the special department, The Krasnodar higher military college of a name of general Shtemenko S.M., academic adviser, Russian Academy of Rocket and Artillery Sciences. Research interests: parallel computations in the residual class system, numerical implementation of the systems of logic algebra functions, functional diagnostics of digital devices with redundant codes, information integrity control in electronic document management systems and other information systems, aspects of the engineering implementation of cryptographic primitives, the number system. The number of publications — 150. ofinko@yandex.ru, http://www.mathnet.ru/eng/person40004; 4, Krasina str., Krasnodar, 350065, Russia; office phone: +79882411171.

Dichenko Sergey Aleksandrovich — Ph.D., lecturer, The Krasnodar higher military college of a name of general Shtemenko S.M.. Research interests: engineering aspects of cryptography: computer algebra, logical calculations in cryptography, error control of cryptographic transformations. The number of publications — 30. dichenko.sa@yandex.ru; 4, Krasina str., Krasnodar, 350065, Russia; office phone: 7-861-268-35-09.

References

1. Kozlitin O.A. [Constructing pseudorandom sequences by means of 2-linear shift register]. *Matematicheskie Voprosy Kriptografii − Mathematical Aspects of Cryptography.* 2014. vol. 9. pp. 632–647. (In Russ.).
2. Hwang T., Gope P. Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network. *Security and communication networks*. 2016. pp. 667–679.
3. Chen D. et al. Multi-message Authentication over Noisy Channel with Secure Channel Codes. 2017. arXiv preprint arXiv:1708.02888. 15 p. Available at: https://arxiv.org/pdf/1708.02888.pdf (accessed: 14.05.2018).
4. Zou M.H., Ma K, Wu K.J. Scan-based attack on stream ciphers: A case study on eSTREAM finalists. Computer science and technology. 2014. vol. 29. pp. 646–655.
5. Yang B., Wu K., Karri R. Scan Based Side Channel Attack on Data Encryption Standart. IACR Cryptology ePrint Archive. 2004. vol. 2004. 6 p. Available at: http://eprint.iacr.org/2004/083.pdf (accessed: 14.05.2018).
6. Hetagurov Ya.A., Prudnev Yu.P. *Povyshenie nadezhnosti cifrovyh ustrojstv metodami izbytochnogo kodirovanija* [Increasing the reliability of digital devices by redundant coding methods]. M.: Jenergija. 1974. 270 p. (In Russ.).
7. Dichenko S.A., Finko O.A. [Safe generators of pseudo-random linear sequences on arithmetic polynomials for secure communication systems]. *Nelineinyi mir – Nonlinear World.* 2013. vol. 9. pp. 632−647. (In Russ.).
8. Finko O.A., Dichenko S.A. Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms: Soft Computing in Computer and Information Science. Soft computing in computer and information science. 2015. vol. 342. pp. 279−290.
9. Tao S., Dubrova E. MVL-PUFs: multiple-valued logic physical unclonable functions. *International Journal of Circuit Theory and Applications*. 2017. vol. 2 no. 45. pp. 292−304.
10. Sokolov A.V., Zhdanov O.N., Ayvazian O.A. [Synthesis methods of algebraic normal form of many-valued logic functions]. *Sistemnyj analiz i prikladnaja informatika – System analysis and applied information science.* 2016. vol. 1. pp. 69−76. (In Russ.).
11. Abd-EI-Barr M., Al-Noori A. Logic Design and Comparison of Arithmetic Structures for AES Cryptographic Systems. International Conference on Security and Management (SAM'2015). 2015. pp. 185−191.
12. Abd-EI-Barr M., Al-Noori A. Arithmetic structures for AES cryptographic systems. 2nd International Conference on Electronics and Communication Systems (ICECS). 2015. pp. 1364−1370.

13. Gardner D., Sălăgean A., Phan R.C.W. Efficient Generation of Elementary Sequences: Cryptography and Coding. IMA International Conference on Cryptography and Coding. 2013. LNCS 8308. pp. 16−27.
14. Kim S-Y., Cho K-R., Lee J-H. Design of *q*-Parallel LFSR-Based Syndrome Generator. *IEICE Transaction on Electronics*. 2015. pp. 594−596.
15. Melnikov S.Yu. [Statistical properties of generalized binary shift registers]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioehlektroniki – Proceedings of Tomsk State University of Control Systems and Radioelectronics.* 2017. vol. 1. pp. 93–95. (In Russ.).
16. Finko O.A., Samoylenko D.V. Parallel generator of *q*-valued pseudorandom sequences based on arithmetic polynomials. *Przeglad Elektrotechniczny*. 2015. vol. 91. no. 3. pp. 24−28.
17. Antonenko V.M., Ivanov A.A., Shmerko V.P. [Linear arithmetic forms of *k*-valued logic functions and their implementation on systolic arrays]. *Avtomatika i telemehanika – Automation and Remote Control*. 1995. vol. 3. pp. 139–155. (In Russ.).
18. Finko O.A. [Modular forms of systems of *k*-valued functions of the algebra of logic]. *Avtomatika i telemehanika – Automation and Remote Control*. 2005. vol. 7. pp. 66–86. (In Russ.).
19. Dziurzanskii P., Malyugin V.D., Shmerko V.P., Yanushkevich S.N. [Linear Models of Circuits Based on the Multivalued Components]. *Avtomatika i telemehanika – Automation and Remote Control.* 2002. vol. 6. pp. 99–119. (In Russ.).
20. Mamontov A.I. [On the Connection between the Functional Systems of Polynomials and Arithmetic Polynomials Representing Systems of Boolean Functions]. *Vestnik Moskovskogo ehnergeticheskogo instituta – Vestnik Moscow Power Engineering Institute.* 2017. vol. 6. pp. 161–165. (In Russ.).
21. Mattoussi F., Roca V., Sayadi B. Complexity Comparison of the Use of Vandermonde versus Hankel Matrices to Build Systematic MDS Reed-Solomon Codes. 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2012. pp. 344–348. Available at: https://arxiv.org/pdf/1708.02888.pdf (accessed: 14.05.2018).
22. Mattoussi F., Khalighi A.M, Bourennane S. Improving the performance of underwater wireless optical communication links by channel coding. *Applied Optics*. 2018. vol. 57. no. 9. pp. 2115–2120.