Нелинейный мир. 2013. №9. С. 632–645

УДК 519-6 (082)

БЕЗОПАСНЫЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЛИНЕЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА АРИФМЕТИЧЕСКИХ ПОЛИНОМАХ ДЛЯ ЗАЩИЩЕННЫХ СИСТЕМ СВЯЗИ

С.А. Диченко, О.А. Финько

Предложена методика повышения безопасности функционирования узлов формирования двоичных псевдослучайных последовательностей (ПСП), действующих в условиях помех, генерируемых злоумышленником. Системы булевых характеристических уравнений реализуются линейными арифметическими полиномами, позволяющими распараллелить процесс вычисления элементов ПСП. «Арифметизация» логического счета, в свою очередь, позволила применить аппарат избыточных арифметических, в частности, модулярных кодов для контроля ошибок функционирования узлов генерации ПСП и обеспечить, тем самым, высокую безопасность их функционирования. Важным преимуществом модулярных кодов является разделение оборудования вычислителя на независимые вычислительные каналы, функционирующие по соответствующим модулям. Такой принцип построения аппаратуры исключает эффект размножения ошибок между каналами и позволяет обеспечить высокую отказоустойчивость генератора ПСП путем реконфигурации оборудования в процессе его функционирования и деградации. Методика предназначена для защищенных систем связи с криптографической защитой информации и систем радиосвязи с расширением спектра сигналов.

Ключевые слова: *безопасность информации, безопасность функционирования криптографических систем, генерация аппаратных ошибок, двоичные псевдослучайные последовательности, контроль ошибок функционирования, линейные рекуррентные регистры сдвига, модулярная*

арифметика, отказоустойчивость, параллельные логические вычисления посредством арифметических полиномов, система остаточных классов, широкополосные системы связи.

SECURE PSEUDORANDOM LINEAR SEQUENCES GENERATORS, BASED ON ARITHMETIC POLYNOMS FOR PROTECTED COMMUNICATION SYSTEMS

S.A. Dichenko, O.A. Finko

The methodology described below is developed for the enhancement of security of functioning of sites of binary pseudorandom sequences (BPS), while operating in “noisy” conditions, invoked by malefactors. The systems of boolean characteristic equations are realized by means of linear arithmetic polynoms, which allow to separate the process of calculation of BPS elements in a way that they all are calculated in parallel. Realization of logical calculations “arithmatization”, in its turn, allowes to apply the means of surplus, in particular modular, codes in order to control operational errors in sites of BPS generation and ensure sites’ enhanced security. An important advantage of modular codes is their ability to separate the data stream through the calculating equipment into independent channels, which function in accordance with their respective modules. The modular design of calculating equipment eliminates the effect of errors’ multiplication between the channels and allows to ensure high fail safety of BPS generator by means of reconfiguration of equipment during operation and in case of obsolescence. Described methodology is intended for protected communication systems with cryptographic data protection mechanisms and for radio communication systems with ability of signal’s rage expansion.

Keywords: *information security, security operation cryptographic systems, generation of hardware errors, pseudo-random binary sequence, the error control function, linear recurrence shift registers, modular arithmetic, fault tolerance, parallel computation by means of logical arithmetic of polynomials, the system of residual classes, broadband communication system.*

Введение

Генераторы линейных ПСП выполняют важную роль при построении систем связи с криптографической защитой информации, защищённых систем радиосвязи с расширением спектра сигналов на основе методов псевдослучайной перестройки рабочей частоты (Frequency Hopping Spread Spectrum), прямой последовательности (Direct Sequence Spread Spectrum) и линейной частотной модуляции (Chirp Spread Spectrum) [1–4].

Из перечня известных атак на средства защиты информации важным является вид атак, основанный на генерации аппаратных ошибок функционирования узлов формирования двоичных ПСП [5]. Для обеспечения необходимого уровня достоверности функционирования [6] цифровых устройств разработано множество методов, наиболее распространенными из которых являются методы резервирования и методы помехоустойчивого кодирования [6–8]. Однако методы резервирования не обеспечивают необходимых уровней достоверности функционирования при ограничениях на аппаратурные затраты, а методы помехоустойчивого кодирования в полной мере не адаптированы к специфике построения и функционирования средств защиты информации (СЗИ), в частности, генераторов ПСП.

Анализ атак, основанных на генерации аппаратных ошибок

В настоящее время рассматриваются атаки на узлы формирования двоичных ПСП посредством [9]:

– анализа результатов измерения потребляемой мощности;

– анализа результатов измерения длительности выполнения операций;

– анализа случайных ошибок функционирования аппаратуры;

– анализа преднамеренно генерируемых аппаратных ошибок и др.

Последние два вида атак пока еще не достаточно хорошо изучены и, поэтому, представляют угрозу информационной безопасности функционирования современным и перспективным средствам защищенной передачи информации. Суть происхождения данного типа атак заключается в использовании тепловых, высокочастотных, ионизирующих или других видов внешних воздействий на СЗИ с целью получения массовых сбоев работы аппаратуры, путем инициирования ошибок вычислений.

Аппаратные атаки можно классифицировать следующим образом.

1. Атаки на оборудование. Последствиями этих атак являются сбои работы СЗИ. Существует возможность анализа последствий данных сбоев. Частный случай этих атак − атаки на средства шифрования. Данный вид атак заключается во внесении искажений битовой информации в определенные места алгоритма преобразований, последствиями которых является возникновение ошибок вычислений, которые в свою очередь могут привести, например, к повторной генерации элементов ПСП, либо генерации ошибочных элементов ПСП, что является недопустимым.

2. Атаки на средства восстановления после сбоев. Некоторые системы не имеют средств восстановления. Если защита разрушена, вернуть программу в работоспособное состояние не представляется возможным. Поэтому подобные системы должны иметь средства противодействия атакам злоумышленника и поддерживать возможность обновления системы безопасности без остановки программы.

Атаки на основе генерации ошибок посредством внешнего воздействия обладают высокой эффективностью для большинства известных и практически используемых в настоящее время алгоритмов генерации ПСП [10–12]. Известно [13], что вероятность генерации ошибки пропорциональна

времени облучения соответствующих регистров, находящихся в благоприятном для возникновения ошибки состоянии, и количеству двоичных разрядов, в пределах которых ожидается ошибка.

Наиболее распространенными и проверенными практикой средствами получения ПСП являются алгоритмы и устройства − линейные рекуррентные регистры сдвига (ЛРРС) − генерации ПСП, основанные на использовании рекуррентных логических выражений [14–19] (рис. 1).

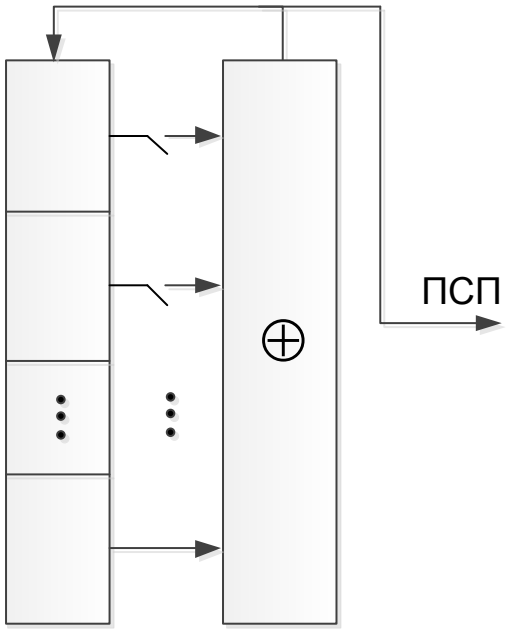


Рисунок 1 – Общий вид ЛРРС

Структура ЛРРС определяется образующим многочленом:

$$D(\chi) = \chi^{\tau} + \chi^{t_l} + \ldots + \chi^{t_2} + \chi^{t_1} + 1,$$

где $\tau, t_i \in N$, а также полученного на его основе характеристического уравнения:

$$\begin{aligned} x_{p+\tau} &= x_p \oplus x_{p+t_1} \oplus x_{p+t_2} \oplus \ldots \oplus x_{p+t_l} \\ &= c_0 x_p \oplus c_1 x_{p+1} \oplus \ldots \oplus c_{\tau-2} x_{p+\tau-2} \oplus c_{\tau-1} x_{p+\tau-1}, \end{aligned} \quad (1)$$

где $x_p, c_i \in \{0,1\}$; $p \in N$; $i = 0, 1, \ldots, \tau - 1$; $c_{i \in \{0, t_1, t_2, \ldots, t_l\}} = 1$.

В терминах линейной алгебры очередной элемент ПСП $x_{p+\tau}$ вычисляется произведением:

$$\begin{Vmatrix} x_{p+\tau} \\ x_{p+\tau-1} \\ \vdots \\ x_{p+2} \\ x_{p+1} \end{Vmatrix} = \begin{Vmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & \cdots & c_{\tau-2} & c_{\tau-1} \end{Vmatrix} \cdot \begin{Vmatrix} x_{p+\tau-1} \\ x_{p+\tau-2} \\ \vdots \\ x_{p+1} \\ x_p \end{Vmatrix}.$$

При реализации атак рассматриваемого вида создаются условия для модификации ПСП или повторной ее генерации.

Пример 1

Генерация ПСП, состоящей из нулевых символов (рис. 2). Результат атаки – передача открытого текста в незащищенный канал связи.

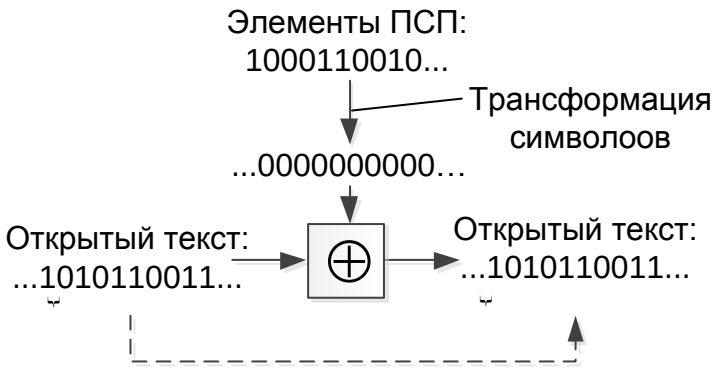


Рисунок 2 – Демонстрация работы узла наложения гаммы шифра при совершении атаки «генерация нулевых символов»

Пример 2

Инициируются ошибки вычисления ПСП. Направление атаки – линейная функция обратной связи, реализуемая через сумматор по модулю два. Например, дан образующий многочлен: $D(\chi) = \chi^4 + \chi + 1$, характеристическое уравнение: $x_{p+4} = x_{p+1} \oplus x_p$, начальное заполнение регистра: $x_p = 1, x_{p+1} = 0, x_{p+2} = 1, x_{p+3} = 0$. Результат атаки – повторная генерация участка ПСП, начиная с 1-го такта работы генератора за счет введения ошибки при вычислении на 9-м такте работы генератора (табл. 1).

Таблица 1 – Состояния ячеек ЛРРС при инициировании ошибки вычислений

№ такта	x_{p+3}	x_{p+2}	x_{p+1}	x_p	Выход ПСП
0	0	1	0	1	1
1	1	0	1	0	0
2	1	1	0	1	1
3	1	1	1	0	0
4	1	1	1	1	1
5	0	1	1	1	1
6	0	0	1	1	1
7	0	0	0	1	1
8	1	0	0	0	0
9	0	1	0	0	0
10	1	0	1	0	0
11	1	1	0	1	1
12	1	1	1	0	0
13	1	1	1	1	1
14	0	1	1	1	1

Пример 3

Генерация ошибки при переходе элемента ПСП от одной к другой ячейки памяти регистра. Направление атаки − процесс перехода элемента ПСП от одной ячейке памяти регистра к другой. Параметры построения регистра соответствуют предыдущему примеру. Начальное заполнение: $x_p = 1, x_{p+1} = 0, x_{p+2} = 0, x_{p+3} = 0$. Результат атаки – повторная генерация участка ПСП, начиная с 5-го такта работы генератора, за счет введения ошибки при переходе элемента ПСП от одной к другой ячейке памяти на 10-м такте работы генератора ПСП (табл. 2). Эффект повторной генерации участка ПСП поясняется с помощью рис. 3.

Таблица 2 – Состояния ячеек ЛРРС при инициировании ошибки сдвига элемента ПСП

№ такта	x_{p+3}	x_{p+2}	x_{p+1}	x_p	Выход ПСП
0	0	0	0	1	1
1	1	0	0	0	0
2	0	1	0	0	0
3	0	0	1	0	0
4	1	0	0	1	1
5	1	1	0	0	0
6	0	1	1	0	0
7	1	0	1	1	1
8	0	1	0	1	1
9	1	0	1	0	0
10	1	1	0	0	0
11	0	1	1	0	0
12	1	0	1	1	1
13	0	1	0	1	1
14	1	0	1	0	0

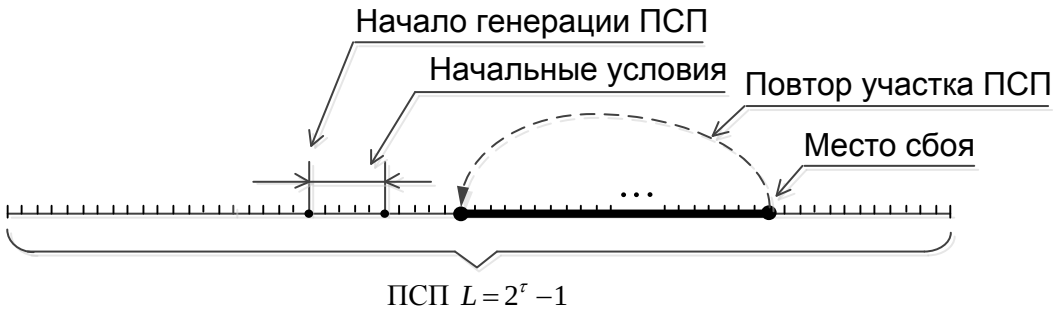


Рисунок 3 – Диаграмма работы генератора ПСП при совершении атаки

Таким образом, атаки, заключающиеся в создании условий возникновения массовых сбоев радиоэлектронной аппаратуры, представляют угрозу безопасности функционирования СЗИ. Одним из путей решения данной проблемы является разработка методов повышения достоверности функционирования узлов СЗИ, наиболее подверженных воздействию атак, рассмотренного вида, в частности узлов гаммообразования, основанных на генерации ПСП.

Анализ путей достоверной генерации двоичных ПСП

В настоящее время необходимый уровень достоверности функционирования узлов формирования двоичной ПСП достигается как за счет привлечения избыточного оборудования (резервирования), так и временной избыточности за счет различного рода повторов вычислений.

В области цифровой схемотехники известны решения, основанные на использовании методов блочного избыточного кодирования [6−8]. Для применения этих методов к генераторам ПСП необходимо предварительно решить задачу распараллеливания процесса вычислений ПСП.

Решение задачи основано на применении классических параллельных алгоритмов вычисления рекурсий [20]. Информационные связи рекурсии (1) можно представить графической зависимостью (рис. 4).

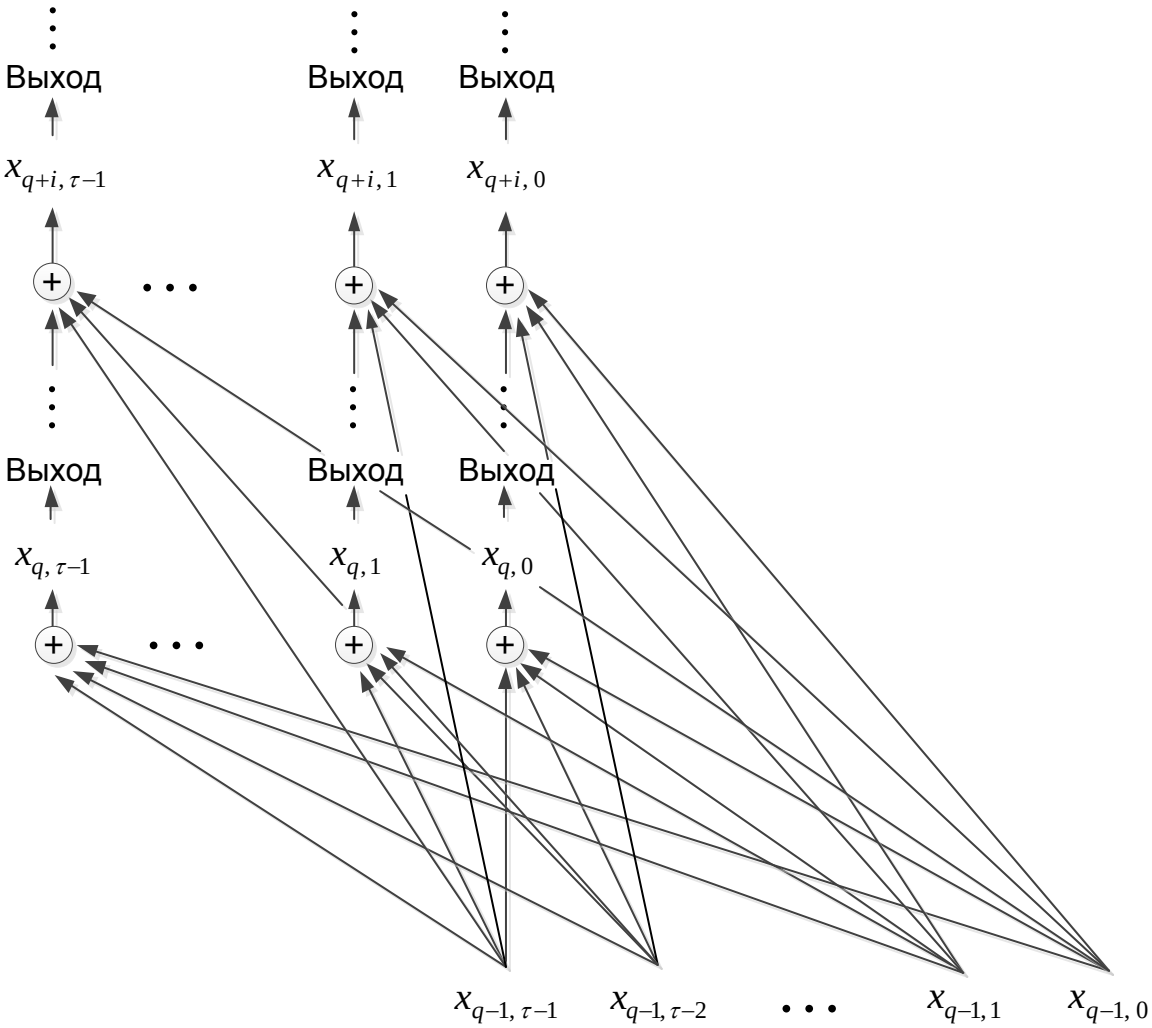


Рисунок 4 – Структура информационных связей рекурсии (1)

Например, для характеристического уравнения:

$$x_{p+\tau} = x_{p+t} \oplus x_p \qquad (2)$$

соответствующего триному $D(\chi) = \chi^\tau + \chi^t + 1$ информационные связи рекурсии (2) характеризуются графической зависимостью, представленной на рис. 5 в соответствии с которой можно построить систему характеристических уравнений:

$$\begin{cases} x_{q,\tau-1} = x_{q-1,\tau-1} \oplus x_{q-1,\tau+t-1}, \\ x_{q,\tau-2} = x_{q-1,\tau-2} \oplus x_{q-1,\tau+t-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{q,1} = x_{q-1,1} \oplus x_{q-1,t+1}, \\ x_{q,0} = x_{q-1,0} \oplus x_{q-1,t}. \end{cases}$$

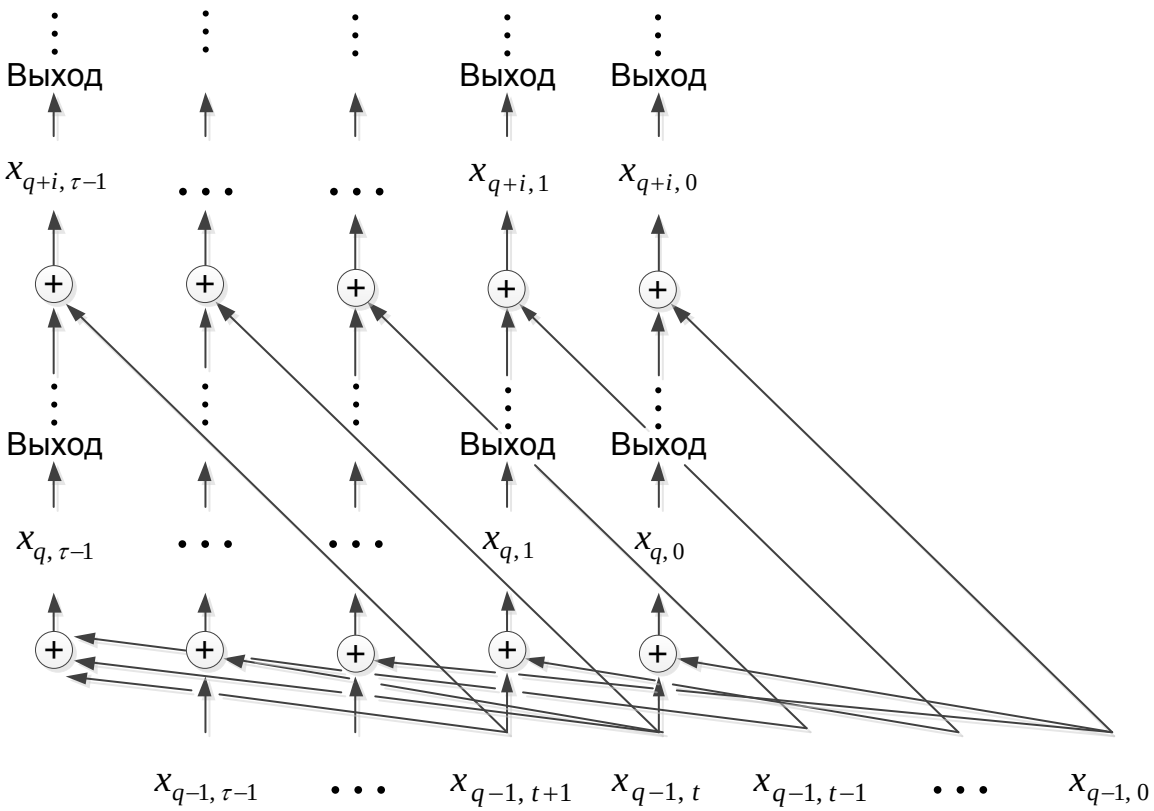


Рисунок 5 – Структура информационных связей рекурсии (2)

Аналогично для общего уравнения (1):

$$\begin{cases} x_{q,\tau-1} = c_0^{(\tau-1)} x_{q-1,0} \oplus c_1^{(\tau-1)} x_{q-1,1} \oplus \ldots \oplus c_{\tau-2}^{(\tau-1)} x_{q-1,\tau-2} \oplus c_{\tau-2}^{(\tau-1)} x_{q-1,\tau-1}, \\ x_{q,\tau-2} = c_0^{(\tau-2)} x_{q-1,0} \oplus c_1^{(\tau-2)} x_{q-1,1} \oplus \ldots \oplus c_{\tau-2}^{(\tau-2)} x_{q-1,\tau-2} \oplus c_{\tau-1}^{(\tau-2)} x_{q-1,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{q,1} = c_0^{(1)} x_{q-1,0} \oplus c_1^{(1)} x_{q-1,1} \oplus \ldots \oplus c_{\tau-2}^{(1)} x_{q-1,\tau-2} \oplus c_{\tau-1}^{(1)} x_{q-1,\tau-1}, \\ x_{q,0} = c_0^{(0)} x_{q-1,0} \oplus c_1^{(0)} x_{q-1,1} \oplus \ldots \oplus c_{\tau-2}^{(0)} x_{q-1,\tau-2} \oplus c_{\tau-1}^{(0)} x_{q-1,\tau-1}, \end{cases} \quad (3)$$

где $c_i^{(j)} \in \{0,1\}$ $(i,\ j = 0,1,\ldots,\tau-1)$.

Система (3) образует информационную матрицу:

$$\mathbf{G}_{\text{инф}} = \begin{Vmatrix} c_0^{(\tau-1)} & c_1^{(\tau-1)} & \cdots & c_{\tau-2}^{(\tau-1)} & c_{\tau-1}^{(\tau-1)} \\ c_0^{(\tau-2)} & c_1^{(\tau-2)} & \cdots & c_{\tau-2}^{(\tau-2)} & c_{\tau-1}^{(\tau-2)} \\ \vdots & \vdots & & \vdots & \vdots \\ c_0^{(1)} & c_1^{(1)} & \cdots & c_{\tau-2}^{(1)} & c_{\tau-1}^{(1)} \\ c_0^{(0)} & c_1^{(0)} & \cdots & c_{\tau-2}^{(0)} & c_{\tau-1}^{(0)} \end{Vmatrix}.$$

Аналогичный результат можно получить другим удобным способом [21]:

$$\mathbf{G}_{\text{инф}} = \begin{Vmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & \cdots & c_{\tau-2} & c_{\tau-1} \end{Vmatrix}^{\tau}.$$

Техника возведения двоичной матрицы в степень может быть выполнена с помощью символических вычислений в любой системе компьютерной алгебры с последующим упрощением (в соответствии с аксиомами алгебры логики) элементов результирующей матрицы вида $Ac_i^k = c_i$ по правилам: 1) $c_i^k = c_i$; 2) $A = 0$, при четном A и $A = 1$, при нечетном A.

Таким образом получим q-й блок ПСП:

$$\mathbf{X}_q = \mathbf{G}_{\text{инф}} \cdot \mathbf{X}_{q-1}.$$

где

$$\mathbf{X}_q = \begin{bmatrix} x_{q,\,\tau-1} & x_{q,\,\tau-2} & \cdots & x_{q,1} & x_{q,0} \end{bmatrix}^{\mathrm{T}},$$

$$\mathbf{X}_{q-1} = \begin{bmatrix} x_{q-1,\,\tau-1} & x_{q-1,\,\tau-2} & \cdots & x_{q-1,1} & x_{q-1,0} \end{bmatrix}^{\mathrm{T}}.$$

Для создания условий применения разделимого линейного избыточного кода получим образующую матрицу $\mathbf{G}_{\text{обр}}$, состоящую из информационной и проверочной матриц путем добавления в (3) проверочных выражений:

$$\begin{cases} x_{q,\,\tau-1} = c_0^{(\tau-1)} x_{q-1,\,0} \oplus c_1^{(\tau-1)} x_{q-1,\,1} \oplus \ldots \oplus c_{\tau-2}^{(\tau-1)} x_{q-1,\,\tau-2} \oplus c_{\tau-1}^{(\tau-1)} x_{q-1,\,\tau-1}, \\ x_{q,\,\tau-2} = c_0^{(\tau-2)} x_{q-1,\,0} \oplus c_1^{(\tau-2)} x_{q-1,\,1} \oplus \ldots \oplus c_{\tau-2}^{(\tau-2)} x_{q-1,\,\tau-2} \oplus c_{\tau-1}^{(\tau-2)} x_{q-1,\,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{q,\,1} = c_0^{(1)} x_{q-1,\,0} \oplus c_1^{(1)} x_{q-1,\,1} \oplus \ldots \oplus c_{\tau-2}^{(1)} x_{q-1,\,\tau-2} \oplus c_{\tau-1}^{(1)} x_{q-1,\,\tau-1}, \\ x_{q,\,0} = c_0^{(0)} x_{q-1,\,0} \oplus c_1^{(0)} x_{q-1,\,1} \oplus \ldots \oplus c_{\tau-2}^{(0)} x_{q-1,\,\tau-2} \oplus c_{\tau-1}^{(0)} x_{q-1,\,\tau-1}, \\ x_{q,\,r-1}^{*} = a_0^{(r-1)} x_{q-1,\,0} \oplus a_1^{(r-1)} x_{q-1,\,1} \oplus \ldots \oplus a_{\tau-2}^{(r-1)} x_{q-1,\,\tau-2} \oplus a_{\tau-1}^{(r-1)} x_{q-1,\,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{q,\,0}^{*} = a_0^{(0)} x_{q-1,\,0} \oplus a_1^{(0)} x_{q-1,\,1} \oplus \ldots \oplus a_{\tau-2}^{(0)} x_{q-1,\,\tau-2} \oplus a_{\tau-1}^{(0)} x_{q-1,\,\tau-1}, \end{cases}$$

где r – количество избыточных символов применяемого линейного кода, $a_i^{(j)} \in \{0, 1\}$ $(i = 0, 1, \ldots, \tau - 1;\ j = 0, \ldots, r - 1;)$.

Образующая матрица примет вид:

$$\mathbf{G}_{\text{обр}} = \begin{Vmatrix} c_0^{(\tau-1)} & c_1^{(\tau-1)} & \cdots & c_{\tau-2}^{(\tau-1)} & c_{\tau-1}^{(\tau-1)} \\ c_0^{(\tau-2)} & c_1^{(\tau-2)} & \cdots & c_{\tau-2}^{(\tau-2)} & c_{\tau-1}^{(\tau-2)} \\ \vdots & \vdots & & \vdots & \vdots \\ c_0^{(1)} & c_1^{(1)} & \cdots & c_{\tau-2}^{(1)} & c_{\tau-1}^{(1)} \\ c_0^{(0)} & c_1^{(0)} & \cdots & c_{\tau-2}^{(0)} & c_{\tau-1}^{(0)} \\ a_0^{(r-1)} & a_1^{(r-1)} & \cdots & a_{\tau-2}^{(r-1)} & a_{\tau-1}^{(r-1)} \\ \vdots & \vdots & & \vdots & \vdots \\ a_0^{(0)} & a_1^{(0)} & \cdots & a_{\tau-2}^{(0)} & a_{\tau-1}^{(0)} \end{Vmatrix}.$$

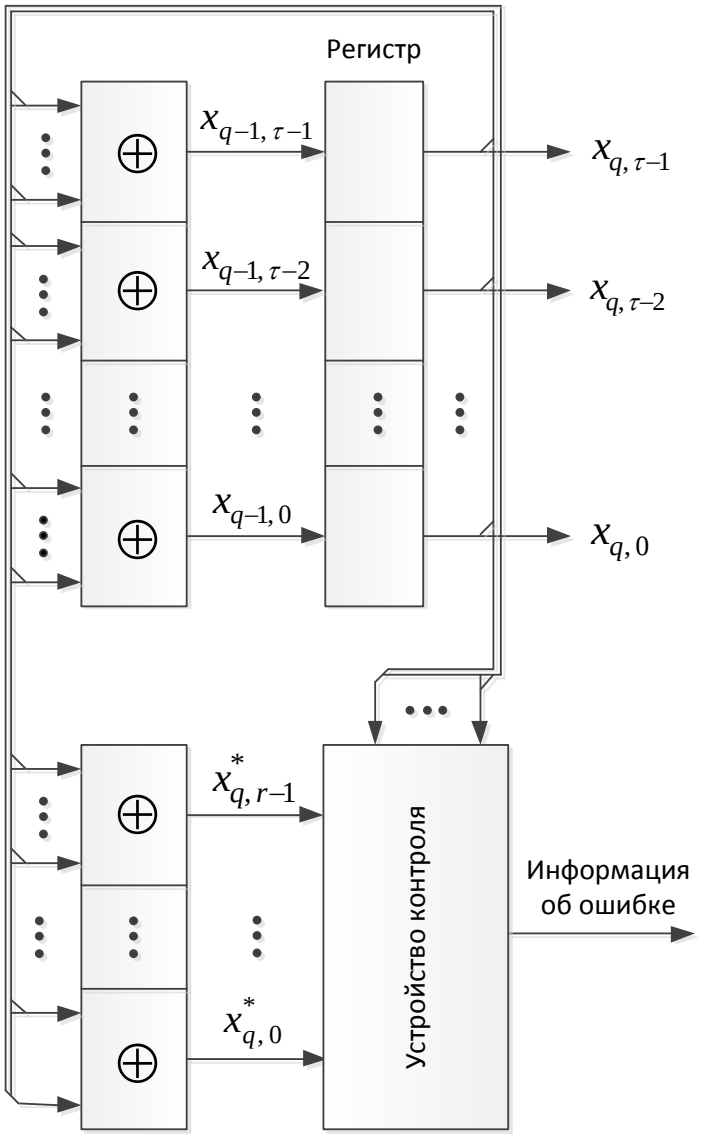
Тогда q -й блок ПСП с контрольными цифрами (блок линейного кода):

$$\mathbf{X}_q^{*} = \begin{bmatrix} x_{q,\,\tau-1} & x_{q,\,\tau-2} & \ldots & x_{q,1} & x_{q,0} & x_{q,\,r-1}^{*} & \ldots & x_{q,\,0}^{*} \end{bmatrix}^{\mathrm{T}}$$

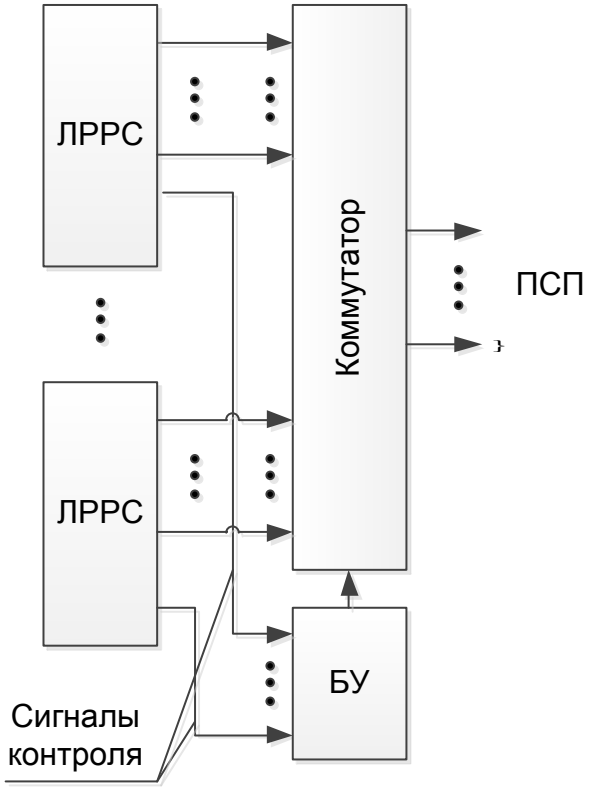
вычисляется путем:

$$\mathbf{X}_q^{*} = \mathbf{G}_{\text{обр}} \cdot \mathbf{X}_{q-1}.$$

Процедура помехоустойчивого декодирования выполняется с помощью известных правил [22]. ЛРРС с встроенной функцией контроля логических вычислений представлен на рисунке 6 а, который может составить основу отказоустойчивого ЛРРС (рис. 6 б).


Регистр
$x_{q-1,\tau-1}$
$x_{q-1,\tau-2}$
$x_{q-1,0}$
$x_{q,\tau-1}$
$x_{q,\tau-2}$
$x_{q,0}$
$x^*_{q,r-1}$
$x^*_{q,0}$
Устройство контроля
Информация об ошибке

а)



б)

Рисунок 6 – а) Общий вид ЛРРС с обнаружением ошибок на основе линейного кода; б) отказоустойчивый ЛРРС на основе ЛРРС с встроенным контролем (БУ – блок управления)

Применение линейных избыточных кодов и методов «горячего» резервирования – не единственный вариант реализации функционального диагностирования и повышения отказоустойчивости цифровых устройств. Важными преимуществами для этих целей обладают арифметические избыточные коды, в частности, так называемые *AN*-коды и коды модулярной арифметики (МА). Применение этих кодов в целях контроля логических типов данных и повышения отказоустойчивости реализующих устройств стало возможным благодаря представлению логических операций арифметическими выражениями [23], в частности ЛЧП и их модулярными формами [24].

Контроль ошибок функционирования генераторов ПСП, основанный на «арифметизации» логического счета

В конце прошлого столетия было сформировано новое направление – параллельные логические вычисления посредством арифметических (числовых) полиномов [23]. Основная заслуга в этом принадлежит сотруднику Института проблем управления РАН им. В.А. Трапезникова профессору В.Д. Малюгину. В последующем это направление получило развитие в различных аспектах в работах проф. В. Шмерко, С. Янушкевич, В. Выхованца, Р. Фараджева, А. Шалыто и др.

При участии авторов в [24–26] были получены положения «Модулярной арифметики параллельных логических вычислений», заключающиеся в объединении теоретических основ машинной МА (часто известна как – система остаточных классов (СОК)) [27–29] и теоретических основ параллельных логических вычислений посредством арифметических полиномов. Цель объединения – использовать достоинства МА, заключающиеся в возможности распараллеливании арифметических вычислений, контроля ошибок вычислений в реальном масштабе времени и обеспечения высокой отказоустойчивости вычислительной аппаратуры, в области параллельного логического счета. И наоборот – развить теорию МА в области параллельных логических вычислений. В последующем данные положения развивались в различных аспектах, в частности, в направлении реализации криптографических функций [30–37]. В частности, в [38, 39[1]] рассматривались параллельные генераторы ПСП, основанные, в общем случае, на нелинейных (канонических) арифметических полиномах. Однако в данном случае применение канонических арифметических полиномов при реализации линейных функций выявило их высокую сложность (длину) . В [33, 34] рассмотрены параллельные генераторы ПСП, основанные на линейных числовых полиномах (ЛЧП), предложенных В.Д. Малюгиным [40],

[1] Опубликовано без ссылки на источник [38] и указания автора идеи, рецензент – к.т.н. Кузьменко А.С.

которые позволили уменьшить максимальную длину реализующего многочлена до величины $n+1$, где n – количество аргументов реализуемой булевой функции. В данной работе этот метод используется как платформа для построения безопасных (самопроверяемых, отказоустойчивых) генераторов ПСП на основе избыточной МА.

Известно [33], что q-й блок участка ПСП можно представить посредством одного ЛЧП. Для этого систему характеристических уравнений (3) необходимо представить, как систему булевых функций, которую в свою очередь, в соответствии с правилами, приведенными в [23, 24, 41] необходимо преобразовать в систему:

$$\begin{cases} L_{\tau-1}(\mathbf{X}_{q-1}) = g_1^{(\tau-1)} x_{q-1,\,0} + g_2^{(\tau-1)} x_{q-1,\,1} + \ldots + g_\tau^{(\tau-1)} x_{q-1,\,\tau-1}, \\ L_{\tau-2}(\mathbf{X}_{q-1}) = g_1^{(\tau-2)} x_{q-1,\,0} + g_2^{(\tau-2)} x_{q-1,\,1} + \ldots + g_\tau^{(\tau-2)} x_{q-1,\,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_0(\mathbf{X}_{q-1}) = g_1^{(0)} x_{q-1,\,0} + g_2^{(0)} x_{q-1,\,1} + \ldots + g_\tau^{(0)} x_{q-1,\,\tau-1}, \end{cases}$$

где $g_j^{(i)}$ (здесь и далее) принимает значение «0» или «1» в зависимости от вхождения в i -й ЛЧП $x_{q-1,\,j}$; $i, j = 0, 1, \ldots, \tau-1$.

Результат вычисления i -того ЛЧП системы представляется двоичным словом длины $l_i = \left\lfloor \log\left(\sum_{j=\tau-1}^{0} g_j^{(i)} \right) \right\rfloor + 1$, где $\lfloor a \rfloor$ – наибольшее целое число. Вычисляется общий ЛЧП:

$$\begin{aligned} & L(\mathbf{X}_{q-1}) = L_{\tau-1}(\mathbf{X}_{q-1}) + 2^{\gamma_1} L_{\tau-2}(\mathbf{X}_{q-1}) + \ldots + 2^{\gamma_{\tau-1}} L_0(\mathbf{X}_{q-1}) = \\ & = g_1^{(\tau-1)} x_{q-1,\,0} + g_2^{(\tau-1)} x_{q-1,\,1} + \ldots + g_\tau^{(\tau-1)} x_{q-1,\,\tau-1} + \\ & + 2^{\gamma_1} \left(g_1^{(\tau-2)} x_{q-1,\,0} + g_2^{(\tau-2)} x_{q-1,\,1} + \ldots + g_\tau^{(\tau-2)} x_{q-1,\,\tau-1} \right) + \ldots \\ & \ldots + 2^{\gamma_{\tau-1}} \left(g_1^{(0)} x_{q-1,\,0} + g_2^{(0)} x_{q-1,\,1} + \ldots + g_\tau^{(0)} x_{q-1,\,\tau-1} \right) = \\ & = h_1 x_{q-1,\,0} + h_2 x_{q-1,\,1} + \ldots + h_\tau x_{q-1,\,\tau-1}, \end{aligned}$$

где $\gamma_k = \sum_{i=0}^{k-1} (l_i + 1)$, $k = 1, 2, \ldots, \tau-1$; $h_j \in Z$, или

$$L(\mathbf{X}_{q-1}) = \sum_{i=1}^{\tau} h_i x_{q-1,\,i-1}. \qquad (4)$$

Окончательный результат образуется путем реализации оператора маскирования $\Xi^{\varphi}\{U\}$, который служит для определения значения φ-ой булевой функции представления $U=(b_{\nu}\ldots b_{\varphi}\ldots b_2 b_1)_2$ (запись $(\ldots)_2$ означает представление целого неотрицательного U в двоичном счислении), то есть $\Xi^{\varphi}\{U\}=b_{\varphi}$. Граф вычисления ЛЧП (4) представлен на рис. 7.

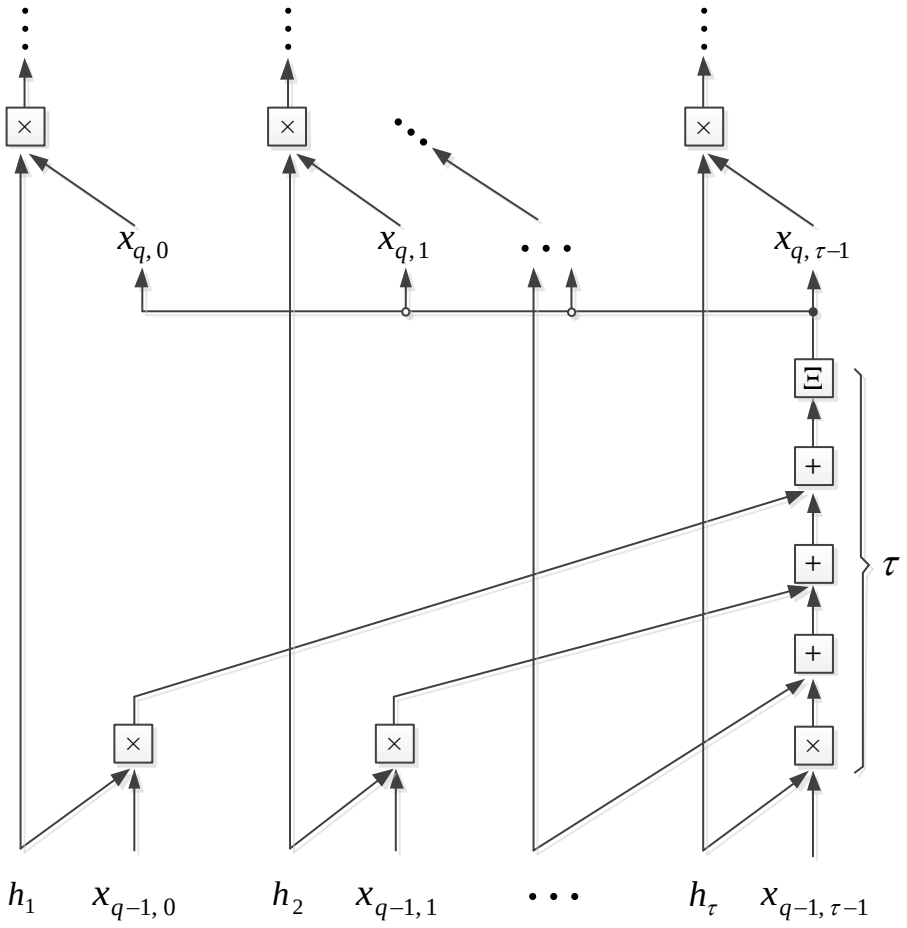


Рисунок 7 – Структура информационных связей ЛЧП (4), где Ξ – оператор маскирования, × – оператор умножения, + – оператор арифметического сложения

В МА целый неотрицательный коэффициент ЛЧП (4) h_j однозначно представляется набором остатков по основаниям МА ($m_1, m_2, \ldots, m_n < m_{n+1} < \ldots < m_k$ – попарно простые):

$$h_j = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_k)_{\text{МА}}, \qquad (5)$$

где $\alpha_t = \left| h_j \right|_{m_t}$; $t = 1, 2, \ldots, n, \ldots, k$; $\left| \bullet \right|_m$ – наименьший неотрицательный вычет числа $\bullet$ по модулю m. Рабочий диапазон $M_n = m_1 m_2 \ldots m_n$ должен удовлетворять $M_n > 2^s$, где $s = \sum\limits_{1 \le \varepsilon \le \tau} l_\varepsilon$ – количество двоичных разрядов, необходимых для представления результата вычисления ЛЧП (4).

Остатки $\alpha_1, \alpha_2, \ldots, \alpha_n$ являются информационными, а $\alpha_{n+1}, \ldots, \alpha_k$ – контрольными. МА в этом случае называется расширенной и охватывает полное множество состояний, представляемых всеми k остатками. Эта область является полным диапазоном МА $[0, M_k)$, где $M_k = m_1 m_2 \ldots m_n m_{n+1} \ldots m_k$, и состоит из рабочего диапазона $[0, M_n)$, определяемого информационными основаниями МА, и диапазона, определяемого избыточными основаниями $[M_n, M_k)$, представляющего недопустимую область для результатов вычислений. Это означает, что операции над числами h_j выполняются в диапазоне $[0, M_k)$. Поэтому, если результат операции МА выходит за пределы M_n, то следует вывод об ошибке вычислений.

Рассмотрим МА, заданную основаниями $m_1, m_2, \ldots, m_n, m_{n+1}$. Каждый коэффициент ЛЧП h_j представим в виде (5) и получим избыточный код МА, представленный системой ЛЧП:

$$\begin{cases} U^{(1)} = L^{(1)}(\mathbf{X}_{q-1}) = \alpha_1^{(1)} x_{q-1,0} + \alpha_2^{(1)} x_{q-1,1} + \ldots + \alpha_\tau^{(1)} x_{q-1,\tau-1}, \\ U^{(2)} = L^{(2)}(\mathbf{X}_{q-1}) = \alpha_1^{(2)} x_{q-1,0} + \alpha_2^{(2)} x_{q-1,1} + \ldots + \alpha_\tau^{(2)} x_{q-1,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ U^{(n)} = L^{(n)}(\mathbf{X}_{q-1}) = \alpha_1^{(n)} x_{q-1,0} + \alpha_2^{(n)} x_{q-1,1} + \ldots + \alpha_\tau^{(n)} x_{q-1,\tau-1}, \\ U^{(n+1)} = L^{(n+1)}(\mathbf{X}_{q-1}) = \alpha_1^{(n+1)} x_{q-1,0} + \alpha_2^{(n+1)} x_{q-1,1} + \ldots + \alpha_\tau^{(n+1)} x_{q-1,\tau-1}. \end{cases} \qquad (6)$$

Подставив в (6) значения остатков МА по соответствующим основаниям для каждого коэффициента (4) и значения переменных

$x_{q-1,0},\ldots,x_{q-1,\tau-1}$, получим значения ЛЧП системы (6), где $U^{(1)},U^{(2)},\ldots,U^{(n)},U^{(n+1)}$ – целые неотрицательные. В соответствии с Китайской теоремой об остатках (КТО) решим систему уравнений:

$$U^*=\left|U^{(1)}\right|_{m_1},U^*=\left|U^{(2)}\right|_{m_2},\ldots,U^*=\left|U^{(n)}\right|_{m_n},U^*=\left|U^{(n+1)}\right|_{m_{n+1}}. \qquad (7)$$

Так как $m_1,m_2,\ldots,m_n,m_{n+1}$ попарно просты, то единственное решением (7) дает выражение:

$$U^*=\left|\sum_{s=1}^{n+1}M_{s,\,n+1}\mu_{s,\,n+1}U^{(s)}\right|_{M_{n+1}}, \qquad (8)$$

где $M_{s,\,n+1}=\dfrac{M_{n+1}}{m_s}$, $\mu_{s,\,n+1}=\left|M_{s,\,n+1}^{-1}\right|_{m_s}$, $M_{n+1}=\prod_{s=1}^{n+1}m_s$.

Вхождение результата вычисления (8) в диапазон (контрольное выражение)

$$0\le U^*<M_n, \qquad (9)$$

означает отсутствие обнаруживаемых ошибок вычислений.

Пример 5

Пусть i-й блок участка двоичной ПСП представлен одним ЛЧП:

$$L(\mathbf{X}_{q-1})=x_{q-1,0}+5x_{q-1,1}+20x_{q-1,2}+80x_{q-1,3}+64x_{q-1,4}.$$

Выберем основания: $m_1=2$, $m_2=3$, $m_3=5$, $m_4=7$, $m_5=11$, $m_6=13$ (m_5,m_6 – контрольные основания). Рабочий и полный диапазоны МА равны: $M_4=m_1m_2m_3m_4=210$ и $M_6=M_4m_5m_6=30030$. Представим каждый коэффициент ЛЧП в МА:

$$\begin{aligned}
h_1=1 &=(1,1,1,1,1,1)_{\text{МА}},\\
h_2=5 &=(1,2,0,5,5,5)_{\text{МА}},\\
h_3=20 &=(0,2,0,6,9,7)_{\text{МА}},\\
h_4=80 &=(0,2,0,3,3,2)_{\text{МА}},\\
h_5=64 &=(0,1,4,1,9,12)_{\text{МА}}.
\end{aligned}$$

Система (6) примет вид:

$$\begin{cases} U^{(1)} = L^{(1)}(x_{q-1,0}, x_{q-1,1}) = x_{q-1,0} + x_{q-1,1}, \\ U^{(2)} = L^{(2)}(x_{q-1,0}, \ldots, x_{q-1,4}) = x_{q-1,0} + 2x_{q-1,1} + 2x_{q-1,2} + 2x_{q-1,3} + x_{q-1,4}, \\ U^{(3)} = L^{(3)}(x_{q-1,0}, x_{q-1,4}) = x_{q-1,0} + 4x_{q-1,4}, \\ U^{(4)} = L^{(4)}(x_{q-1,0}, \ldots, x_{q-1,4}) = x_{q-1,0} + 5x_{q-1,1} + 6x_{q-1,2} + 3x_{q-1,3} + x_{q-1,4}, \\ U^{(5)} = L^{(5)}(x_{q-1,0}, \ldots, x_{q-1,4}) = x_{q-1,0} + 5x_{q-1,1} + 9x_{q-1,2} + 3x_{q-1,3} + 9x_{q-1,4}, \\ U^{(6)} = L^{(6)}(x_{q-1,0}, \ldots, x_{q-1,4}) = x_{q-1,0} + 5x_{q-1,1} + 7x_{q-1,2} + 2x_{q-1,3} + 12x_{q-1,4}. \end{cases}$$

Пусть $x_{q-1,0}=1$, $x_{q-1,1}=0$, $x_{q-1,2}=1$, $x_{q-1,3}=0$, $x_{q-1,4}=1$. Тогда $U^{(1)}=1$, $U^{(2)}=4$, $U^{(3)}=5$, $U^{(4)}=8$, $U^{(5)}=19$, $U^{(6)}=20$. Решив с помощью (8) систему:

$$U^* = |1|_2, U^* = |4|_3, U^* = |5|_5, U^* = |8|_7, U^* = |19|_{11}, U^* = |20|_{13}, \qquad (10)$$

получим: $U^*=85$. Так как $85<210$, то в соответствии с контрольным отношением (9) следует вывод об отсутствии обнаруживаемых ошибок вычислений. Значения ЛЧП (4) получим, подставив значения булевых переменных: $U=1+5\cdot 0+20\cdot 1+80\cdot 0+64\cdot 1=85$.

Реконфигурация оборудования

Восстановление достоверного функционирования генератора ПСП в случае возникновения долговременного отказа возможно путем исправления ошибки или реконфигурации оборудования генератора (активного резервирования). Первый вариант является неприемлемым, так как не гарантирует не проникновения необнаруживаемых ошибок в результат шифрования. Благодаря применению методов избыточного модулярного кодирования стало возможным применить вариант реконфигурации оборудования путем исключения из процесса функционирования отказавшего оборудования [42].

После локализации неисправного оборудования – например − одного канала функционирования МА, операция реконфигурации выполняется вычислением U^* из системы:

$$U^* = \left|U^{(1)}\right|_{m_1}, \ldots, U^* = \left|U^{(n)}\right|_{m_n}, U^* = \left|U^{(n+1)}\right|_{m_{n+1}}, U^* = \left|U^{(n+2)}\right|_{m_{n+2}}$$

по «правильным» основаниям МА:

$$U^* = \left|\tilde{U}^{(1)} B_{1,j} + \tilde{U}^{(2)} B_{2,j} + \ldots + \tilde{U}^{(n+2)} B_{n+2,j}\right|_{M_j}, \qquad (11)$$

где $\tilde{U}^{(i)}$ – ошибочный остаток; $B_{i,j}$ – ортогональные базисы; $i, j = 1, 2, \ldots, n+2$; $i \neq j$; $B_{i,j} = \dfrac{M_j \mu_{i,j}}{m_i}$; $M_j = \dfrac{M_{n+2}}{m_j}$; $\mu_{i,j}$ вычисляется из сравнения: $\dfrac{M_j \mu_{i,j}}{m_i} \equiv 1 \mod m_i$. Составляется таблица 3, содержащая значения ортогональных базисов и модулей системы для условий возникновения однократной ошибки по каждому основанию МА.

Таблица 3 – Расчетная таблица ортогональных базисов и модулей системы

j	$B_{1,j}$	$B_{2,j}$	…	$B_{n+2,j}$	M_j
1	0	$\dfrac{M_1 \mu_{2,1}}{m_2}$	…	$\dfrac{M_1 \mu_{n+2,1}}{m_{n+2}}$	$m_2 m_3 \ldots m_{n+2}$
2	$\dfrac{M_2 \mu_{1,2}}{m_1}$	0	…	$\dfrac{M_2 \mu_{n+2,2}}{m_{n+2}}$	$m_1 m_3 \ldots m_{n+2}$
⋮	⋮	⋮	⋱	⋮	⋮
$n+2$	$\dfrac{M_{n+2} \mu_{1,n+2}}{m_1}$	$\dfrac{M_{n+2} \mu_{2,n+2}}{m_2}$	…	0	$m_1 m_2 \ldots m_{n+1}$

Пример 6

Допустим, что при вычислении решения системы (10) обнаружена ошибка, например, по основанию m_2. В соответствии с (11) вычислим U^*, используя табл. 3. Получим:

$$U^* = \left|U^{(1)}B_{1,j} + \tilde{U}^{(2)}B_{2,j} + \ldots + U^{(6)}B_{6,j}\right|_{M_2} = \left|1\cdot B_{1,j} + \tilde{U}^{(2)}\cdot 0 + \ldots + 20\cdot B_{6,j}\right|_{M_2} =$$

$$= \left|1\cdot B_{1,j} + 5\cdot B_{3,j} + 8\cdot B_{4,j} + 19\cdot B_{5,j} + 20\cdot B_{6,j}\right|_{M_2} = 85.$$

Структурная схема безопасного генератора ПСП представлена на рис. 8.

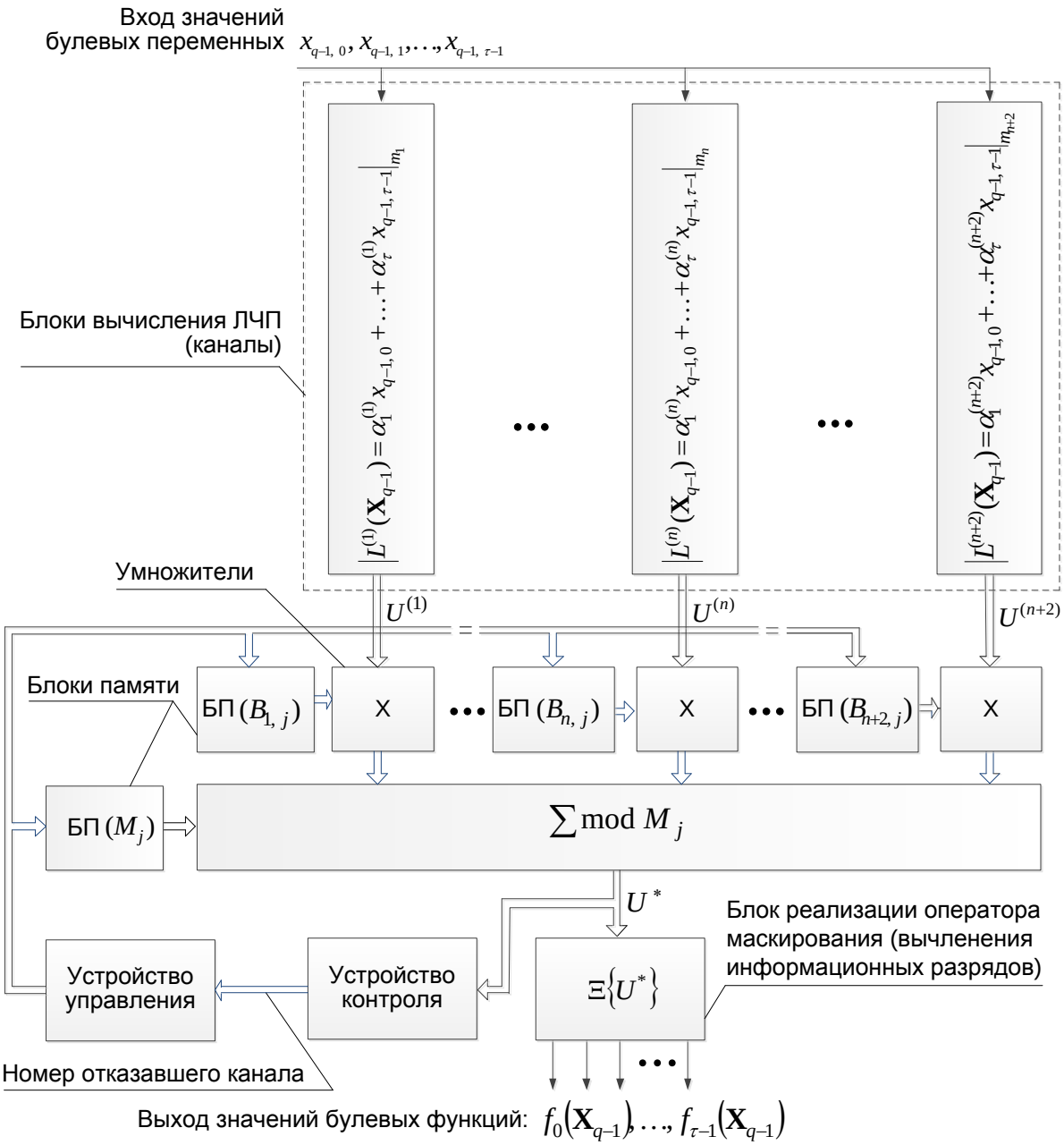


Рисунок 8 – Структурная схема безопасного генератора ПСП

Заключение

Известно, что применение МА уже с двумя избыточными основаниями позволяет обеспечить уровень отказоустойчивости модулярного вычислителя, превосходящую отказоустойчивость, обеспечиваемую методом троирования оборудования. При этом избыточные аппаратурные затраты сокращаются с 200% (при троировании) до 30−40% (при использовании МА) [30]. В тоже время следует отметить, что объем оборудования построенного устройства (рис. 8) может превышать (зависит от применяемых технических решений) объем оборудования отказоустойчивого ЛРРС (рис. 6б). Поэтому следует учитывать принципиально новый достигнутый уровень функциональной гибкости данного устройства, способного реализовывать и множество других криптографических функций, изменяющихся во времени, без перестройки его структуры [27, 32]. Это позволяет использовать для реализации устройства не только ПЛИС, но и высокотехнологичные заказные БИС, в частности уже применяющиеся для реализации теоретико-числовых преобразований в области цифровой обработки сигналов [43].

Реализация генераторов ПСП с помощью ЛЧП и избыточной МА позволяет получить новый класс решений, направленных на безопасную реализацию логических криптографических функций, в частности параллельных генераторов ПСП. При этом обеспечивается как функциональный контроль оборудования (в реальном масштабе времени, что принципиально для СЗИ), так и его отказоустойчивость за счет реконфигурации структуры вычислителя в процессе ее деградации. При необходимости, вопросы тестового диагностирования могут быть решены на основе известных решений [44]. Классический ЛРРС, рассмотренный в настоящей работе, составляет основу и более сложных, например, комбинирующих генераторов ПСП [18]. Использование для реализации генератора ПСП модулярных арифметических вычислений обеспечивает возможность применения предложенных решений в составе гибридных

криптосистем (включающих ассиметричные) [32]. При этом арифметический вычислитель, поддерживающий реализацию ассиметричного шифра, используется для реализации булевых функций (элементов ПСП).

Литература

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 349 с.

2. Варакин Л.Е. Теория систем сигналов. М.: Совет. радио, 1978. 219 с.

3. Борисов В.И., Зинчук В.М., Лимарев А.Е., Мухин Н.П., Шестопалов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2000. 384 с.

4. Борисов В.И., Зинчук В.М., Лимарев А.Е., Шестопалов В.И. Помехозащищённость систем радиосвязи с расширением спектра прямой модуляцией псевдослучайной последовательностью. М.: РадиоСофт, 2011. 550 с.

5. Yang B., Wu K., Karri R. Scan Based Side Channel Attack on Data Encryption Standard // Report 2004/324, http://eprint.iacr.org, 2004. P. 114–116.

6. Щербаков Н.С. Достоверность работы цифровых устройств. М.: Машиностроение, 1989. 224 с.

7. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. М.: Радио и связь, 1989. 208 с.

8. Хетагуров Я.А., Пруднев Ю.П. Повышение надежности цифровых устройств методами избыточного кодирования. М.: Энергия, 1974. 272 с.

9. Kelsey J. Protocol Interactions and the Chosen Protocol Attack // Security Protocols, 5th Int'l Workshop, Springer-Verlag, New York. 1996, P. 91–104.

10. Canovas C., Clediere J. What do DES S-boxes Say in Differential Side Channel Attacks? // Report 2005/311, http://eprint.iacr.org, 2005. P. 191–200.

11. Carlier V., Chabanne H., Dottax E. Electromagnetic Side Channels of an FPGA Implementation of AES // Report 2004 / 145, http://eprint.iacr.org, 2004. P. 111–124.

12. Page D. Partitioned Cache Architecture as a Side-Channel Defence Mechanism // Report 2005/280, http://eprint.iacr.org, 2005. P. 213–225.

13. Gutmann P. Software Generation of Random Numbers for Cryptographic Purposes // Usenic Security Symp., Usenix Assoc., Berkeley, Calif, 1998. P. 243–257.

14. Бабаш А.В., Шанкин Г.П. Криптография. М.: Солон-Р, 2002. 512 с.

15. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Псевдослучайные и полилинейные последовательности. Труды по дискретной информации, том 1. М.: ТВП. 1997. С. 139–202.

16. Куракин В.Л. Полиномиальные преобразования линейных рекуррентных последовательностей над конечными коммутативными кольцами // Дискрет. мат. 2000. № 3. С. 3–36.

17. Песошин В.А., Кузнецов В.М. Генераторы псевдослучайных и случайных чисел на регистрах сдвига: моногр. Казань: Изд-во Казан. Гос.техн.ун-та, 2007. 296 с.

18. Шнайер Б. Практическая криптография. М.: Вильямс, 2005. 424 с.

19. Фороузан Б.А. Криптография и безопасность сетей: учебное пособие / пер. с англ. под ред. А.Н. Берлина. М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. 784 с.

20. Ортега Дж. Введение в параллельные и векторные методы решения линейных систем. М.: Мир, 1991. 365 с.

21. Klein A. Stream Ciphers. Springer, http://www.springer.com, 2013, 399 p.

22. Хэмминг Р.В. Теория кодирования и теория информации. М.: Радио и связь, 1983. 173 с.

23 Малюгин В.Д. Параллельные логические вычисления посредством арифметических полиномов. М.: ФИЗМАТЛИТ, 1997. 192 с.

24. Финько О.А. Реализация систем булевых функций большой размерности методами модулярной арифметики // Автоматика и телемеханика. 2004. № 6. С. 37–60.

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

26. Финько О.А. Модулярная арифметика параллельных логических вычислений. М.: ИПУ РАН, 2003. 224 с.

27. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. М.: Совет. радио, 1968. 440 с.

28. Амербаев В.М. Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 324 с.

29. Торгашев В.А. Система остаточных классов и надежность ЦВМ. М.: Совет. радио, 1973. 120 с.

30. Вишневский А.К., Шарай В.А. Реализация операций подстановки линейными числовыми полиномами // Известия ЮФУ. Технические науки. 2010. № 4. С. 110–117.

31. Вишневский А.К., Финько О.А. Реализация типовых функций гибридных криптосистем арифметико-логическими полиномами // Теория и техника радиосвязи. 2011. № 1. С. 51–60.

32. Вишневский А.К., Финько О.А. Параллельная реализация систем подстановок числовыми полиномами // Труды пятой международной конференции «Параллельные вычисления и задачи управления (PACO’2010)». Москва. 26-28 октября 2010 г. ИПУ РАН им. В.А. Трапезникова. Москва. С.112–120.

33. Диченко С.А., Вишневский А.К., Финько О.А. Реализация двоичных псевдослучайных последовательностей линейными числовыми полиномами // Известия ЮФУ. Технические науки. 2011. № 12. С. 130–140.

34. Финько О.А., Диченко С.А., Вишневский А.К. Самопроверяемый специализированный вычислитель систем булевых функций // Патент России № 2485575, 20.06.2013.

35. Финько О.А., Вишневский А.К., Диченко С.А., Самойленко Д.В. и др. Арифметический вычислитель систем булевых функций // Патент России № 2461868, 20.09.2012.

36. Финько О.А., Сульгин С.М., Щербаков А.В. и др. Самопроверяемый модулярный вычислитель систем логических функций // Патент России № 2417405, 27.04.2011.

37. Финько О.А., Щербаков А.В. Модулярный вычислитель систем логических функций // Патент России № 2417303, 16.11.2009.

38. Сизоненко А.Б., Финько О.А. Арифметические модели типовых узлов криптографических средств защиты информации в кн. Криптографические методы защиты информации, кн. 4, гл. 5, Научная серия: «Защита информации», ред. Е.М. Сухарев, Радиотехника. М., 2007. С.74–90.

39[2]. Сизоненко А.Б. Параллельная реализация рекуррентного регистра сдвига на основе представления систем логических функций арифметическими полиномами // Теория и техника радиосвязи. 2012. № 3. С. 111–116.

40. Шмерко В.П. Теоремы Малюгина: новое понимание в логическом управлении, проектировании СБИС и структурах данных для новых технологий // Автоматика и телемеханика. 2004. № 6. С. 61–83.

41. Yanushkevich L., Shmerko V., Lyshevski S. Logic design of nanoICs. CRC Press, 2005. 459 p.

42. Иыуду А.К. Надежность, контроль и диагностика вычислительных машин и систем: учеб. пособие для вузов по спец. «Вычислительные машины, комплексы, системы и сет». М.: Высш. шк., 1989. 216 с.

[2] Опубликовано без ссылки на источник [38] и указания автора идеи, рецензент – к.т.н. Кузьменко А.С.

43. Omondi A., Premkumar B. Residue Number System: Theory and Implementation. London: Imperial Collegt Press, 2007. 296 p.

44. Долгов А.И. Диагностика устройств, функционирующих в системе остаточных классов. М.: Радио и связь, 1982. 64 с.

Диченко Сергей Александрович − (1986), адъюнкт Военной академии связи.

Область научных интересов: параллельные самоконтролируемые генераторы псевдослучайных чисел и двоичных последовательностей их применение в защищённых системах связи.

E-mail: dichenko.sa@yandex.ru.

Финько Олег Анатольевич − (1963), докт. техн. наук, профессор кафедры филиала Военной академии связи (г. Краснодар).

Область научных интересов: модулярная арифметика, параллельные логические вычисления, криптографическая защита информации.

E-mail: ofinko@yandex.ru; URL: http://ofinko.ru/

Dichenko Sergey − (1986), an associate of the Military Academy of Communications.

Research interests: self-controlled parallel pseudo-random binary sequence of numbers and their application in secure communication systems.

E-mail: dichenko.sa@yandex.ru.

Finko Oleg − (1963), Doctor. tehn. Sciences, Department of the branch of the Military Academy of Communications (Krasnodar).

Research interests: modular arithmetic, logical parallel computing, cryptographic protection of information.

E-mail: ofinko@yandex.ru; URL: http://ofinko.ru/