РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 579 991** (13) **C1**

(51) МПК
G06F 7/57 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2015116042/08, 27.04.2015

(24) Дата начала отсчета срока действия патента:
27.04.2015

Приоритет(ы):
(22) Дата подачи заявки: 27.04.2015

(45) Опубликовано: 10.04.2016 Бюл. № 10

(56) Список документов, цитированных в отчете о поиске: RU 2373564 C2, 20.11.2009. RU 2485575 C1, 10.05.2014. RU 2485575 C1, 20.06.2013. GB 2342732 A, 19.04.2000.

Адрес для переписки:
350063, г. Краснодар, ул. Красина, 4, Краснодарское высшее военное училище

(72) Автор(ы):
Диченко Сергей Александрович (RU),
Крупенин Александр Владимирович (RU),
Финько Олег Анатолиевич (RU),
Самойленко Дмитрий Владимирович (RU),
Чечин Иван Владимирович (RU),
Меретуков Клим Сергеевич (RU),
Самус Владимир Михайлович (RU)

(73) Патентообладатель(и):
федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище имени генерала армии С.М. Штеменко" Министерства обороны Российской Федерации (RU)

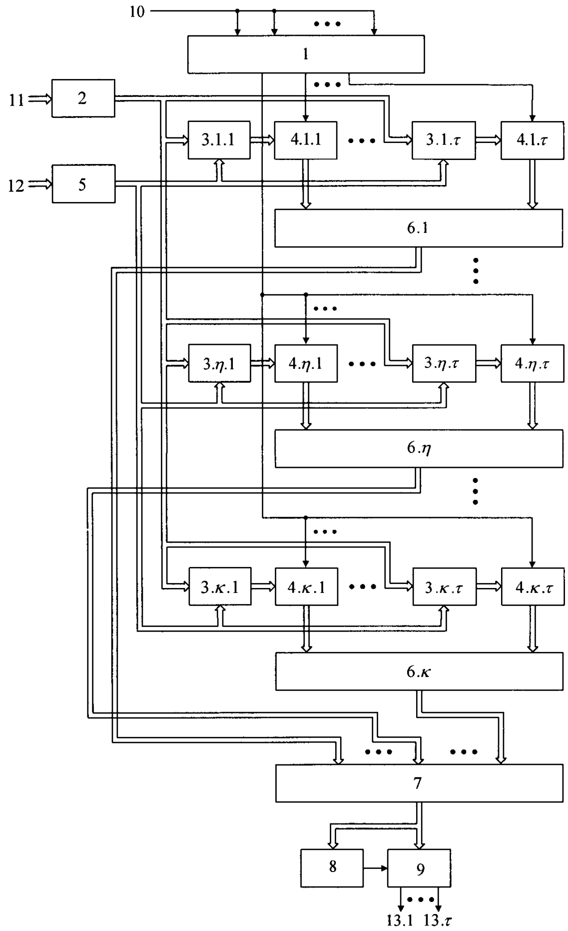
(54) САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ

(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано для параллельной реализации систем булевых функций с функцией обеспечения контроля ошибок вычислений в средствах криптографической защиты информации. Техническим результатом является расширение функциональных возможностей устройства за счет обеспечения возможности достоверного вычисления двоичных псевдослучайных последовательностей, идентичных псевдослучайным последовательностям, получаемым посредством классических генераторов на линейных рекуррентных регистрах сдвига. Устройство обеспечивает вычисление системы булевых функций, представленной в числовой форме, посредством применения избыточных модулярных кодов и дополнительно содержит регистр памяти, блок памяти хранения оснований системы, блоки вычисления наименьших неотрицательных вычетов числа по основаниям системы, множители, многоместные сумматоры, блок решения системы сравнений с одним неизвестным, блок сравнения, блок оператора маскирования. 7 ил.

RU 2579991 C1

RU 2579991 C1



Фиг. 1

RU 2579991 C1

RU 2579991 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 579 991** (13) **C1**

(51) Int. Cl.
G06F 7/57 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: 2015116042/08, 27.04.2015

(24) Effective date for property rights:
27.04.2015

Priority:
(22) Date of filing: 27.04.2015

(45) Date of publication: 10.04.2016 Bull. № 10

Mail address:
350063, g. Krasnodar, ul. Krasina, 4, Krasnodarskoe vysshee voennoe uchilishche

(72) Inventor(s):
Dichenko Sergej Aleksandrovich (RU),
Krupenin Aleksandr Vladimirovich (RU),
Finko Oleg Anatolievich (RU),
Samojlenko Dmitrij Vladimirovich (RU),
CHechin Ivan Vladimirovich (RU),
Meretukov Klim Sergeevich (RU),
Samus Vladimir Mikhajlovich (RU)

(73) Proprietor(s):
federalnoe gosudarstvennoe kazennoe voennoe obrazovatelnoe uchrezhdenie vysshego obrazovanija "Krasnodarskoe vysshee voennoe uchilishche imeni generala armii S.M. SHtemenko" Ministerstva oborony Rossijskoj Federatsii (RU)

(54) SELF-CHECKING SPECIAL-PURPOSE COMPUTER OF BOOLEAN FUNCTION SYSTEMS

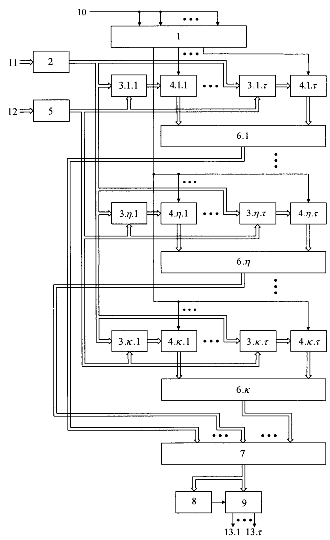
(57) Abstract:

FIELD: computer engineering.

SUBSTANCE: invention relates to computer engineering and can be used for parallel implementation systems Boolean functions with a function of control computation errors in means of cryptographic information protection. Device provides calculation system of Boolean functions, presented in a numerical form, by applying excessive code modular and additionally contains a memory register, a memory unit storing bases system, units for calculating the least non-negative residue number at the bases of the system, multipliers, multi-bed adders, a decision system comparisons with one unknown, comparison unit, unit of the operator masking.

EFFECT: technical result is expansion of device functional capabilities by enabling accurate calculation of binary pseudorandom sequences, identical pseudo-random sequences obtained by means of classical generators on linear recurrent shift registers.

1 cl, 7 dwg



Фиг. 1

RU 2579991 C1

RU 2579991 C1

Предлагаемое устройство относится к вычислительной технике и может быть использовано для параллельной реализации систем булевых функций с функцией обеспечения контроля ошибок вычислений в средствах криптографической защиты информации.

Известно вычислительное устройство, содержащее шифраторы, выходы которых подключены к входам устройств сравнения, выходы которых подключены к входам устройства управления, выходы которого подключены к постоянным запоминающим устройствам (ПЗУ), предназначенным для хранения констант ортогональных базисов и общего модуля системы, выходы которых подключены к входам умножителей, к которым также подключены выходы шифраторов, на входы которых поступают значения наименьших неотрицательных вычетов по системе попарно простых и упорядоченных модулей системы, значения первого из которых поступают на вход первого умножителя и входы устройств сравнения. Выходы умножителей и выход ПЗУ, предназначенного для хранения констант общего модуля системы, подключены к входам сумматора по общему модулю, выход которого является шиной выдачи результата вычислений (Финько, О.А. Контроль и реконфигурация аналого-цифровых устройств, функционирующих в системе остаточных классов / О.А. Финько // Электронное моделирование. Том №22.4.2000. - С. 92-103).

Недостаток известного устройства - отсутствие функциональных возможностей безошибочного (достоверного) вычисления двоичных псевдослучайных последовательностей, идентичных псевдослучайным последовательностям, получаемым посредством классических генераторов на линейных рекуррентных регистрах сдвига.

Наиболее близким по сущности технического решения заявленному устройству является вычислительное устройство, включающее в себя блоки памяти, предназначенные для хранения коэффициентов полиномов избыточной числовой нормальной формы, входы которых являются входами устройства, к которым подключена шина подачи булевых переменных, выходы которых соединены с входами многоместных сумматоров, выходы которых соединены с информационными входами многоканальных мультиплексоров, выходы первого мультиплексора подключены к входам блока вычисления остатка по модулю и информационным входам регистра памяти, выходы которого являются выходами устройства выдачи значений булевых функций, выходы второго мультиплексора подключены к входам блока вычисления остатка по модулю, выходы которого подключены к входам элемента ИЛИ-НЕ, выход которого подключен к первому входу элемента И, второй вход которого подключен к входу подачи синхроимпульсов устройства, а выход - подключен к синхровходу регистра памяти; шина подачи коэффициентов полинома избыточной числовой нормальной формы подключена к входам блоков памяти; блок памяти хранения адресов информационных разрядов, к входу которого подключена шина адреса, выход которого подключен к адресным входам мультиплексоров (Пат. 2485575 Российская Федерация, МПК^{12} G06F 7/57. Самопроверяемый специализированный вычислитель систем булевых функций [Текст] / О.А. Финько, С.А. Диченко, А.К. Вишневский. - №2012120739; заявл. 18.05.2012; зарегистр. 20.06.2013 - 14 с.: ил.).

Недостаток известного устройства - отсутствие функциональных возможностей безошибочного (достоверного) вычисления двоичных псевдослучайных последовательностей, идентичных псевдослучайным последовательностям, получаемым посредством классических генераторов на линейных рекуррентных регистрах сдвига.

Цель изобретения - расширение функциональных возможностей устройства за счет обеспечения возможности безошибочного (достоверного) вычисления двоичных псевдослучайных последовательностей, идентичных псевдослучайным последовательностям, получаемым посредством классических генераторов на линейных рекуррентных регистрах сдвига.

Поставленная цель достигается тем, что в самопроверяемый специализированный вычислитель систем булевых функций, содержащий шину подачи τ булевых переменных, блок памяти, предназначенный для хранения коэффициентов линейного числового полинома, к входу которого подключена шина подачи коэффициентов; дополнительно введены регистр памяти, входы которого являются входами устройства, к которым подключена шина подачи τ булевых переменных; блок памяти, предназначенный для хранения оснований системы, к входу которого подключена шина подачи оснований системы, выходы которого вместе с выходами блока памяти хранения коэффициентов линейного числового полинома подключены к входам блоков вычисления наименьших неотрицательных вычетов числа (коэффициентов линейного числового полинома) по основаниям системы, выходы которых вместе с выходами регистра памяти подключены к входам множителей, выходы которых подключены к входам многоместных сумматоров, выходы которых подключены к входам блока решения системы сравнений с одним неизвестным, выход которого подключен к входам блока сравнения и блока оператора маскирования, выход блока сравнения подключен ко второму входу блока оператора маскирования, выходы которого являются выходами устройства выдачи значений τ булевых функций.

Структурная схема предлагаемого устройства дана на фиг. 1.

Предлагаемое устройство предназначено для вычисления двоичных псевдослучайных последовательностей (ПСП), идентичных ПСП, получаемым посредством классических генераторов на линейных рекуррентных регистрах сдвига (ЛРРС), с функцией осуществления контроля ошибок вычислений. Работа устройства основана на представлении систем рекурсивных характеристических уравнений линейными числовыми полиномами (ЛЧП).

Алгоритмы и устройства генерации ПСП, основанные на использовании рекуррентных логических выражений и неприводимых полиномов, наиболее простым по структуре из которых является ЛРРС (фиг. 2), считаются наиболее распространенными и проверенными практикой (Бабаш, А.В. Криптография / А.В. Бабаш, Г.П. Шанкин. - М.: СОЛОН-Р, 2002. - 575 с.).

Структура ЛРРС определяется образующим многочленом:

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

где τ, $t_i \in N$ ($i=1, 2, \ldots, l$), а также полученным на его основе характеристическим уравнением:

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

где x_p, x_{p+t_i}, $c_j \in \{0, 1\}$; $p \in N$; $j=0, 1, \ldots, \tau-1$; $c_{j\in\{0,t_1,t_2,\ldots,t_l\}} = 1$.

В терминах линейной алгебры очередной элемент ПСП $x_{p+\tau}$ вычисляется произведением (Песошин, В.А. Генераторы псевдослучайных и случайных чисел на регистрах сдвига: моногр. / В.А. Песошин, В.М. Кузнецов. - Казань: Казан. гос. техн. ун-т, 2007. - 296 с.):

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

Для осуществления контроля ошибок вычислений в области цифровой схемотехники известны решения, основанные на использовании методов избыточного модулярного кодирования (Согомонян, Е.С. Самопроверяемые устройства и отказоустойчивые системы [Текст] / Е.С. Согомонян, Е.В. Слабаков. - М.: Радио и связь, 1989. - 208 с.). 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 (Ортега, Дж. Введение в параллельные и векторные методы решения линейных систем [Текст] / Дж. Ортега. - М.: Мир, 1991. - 365 с.). Так, например, информационные связи рекурсии (1) можно представить графической зависимостью (фиг. 3).

В частности, ЛРРС длины τ , реализующий данный метод, имеет r ячеек памяти, значения которых совместно образуют (начальное) состояние $(x_{q-1,0}, \dots, x_{q-1,t}, \dots, x_{q-1,\tau-1})$. После первого такта работы ЛРРС выдаст $x_{q-1,0}$ и перейдет в состояние $(x_{q-1,1}, \dots, x_{q,0})$, где $x_{q,0}=x_{q-1,0} \oplus x_{q-1,t}$. Продолжая таким образом, ЛРРС генерирует ПСП. Общий вид данного ЛРРС представлен на фиг. 4.

Так, например, для характеристического уравнения:

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

где $x_{p+\tau}, x_{p+t}, x_p \in \{0,1\}$, соответствующего триному $D(x)=\chi^\tau+\chi^t+1$ (где τ - степень тринома; $\tau, t \in N$; $\tau \geq 3$; $1 \leq t \leq \tau-1$), информационные связи рекурсии (2) характеризуются графической зависимостью, представленной на фиг. 5, в соответствии с которой можно построить систему характеристических уравнений (3):

$$\begin{cases} x_{q,\tau-1} = x_{q-1,\tau-1} \oplus x_{q-1,\tau+t-1}, \\ x_{q,\tau-2} = x_{q-1,\tau-2} \oplus x_{q-1,\tau+t-2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x_{q,0} = x_{q-1,0} \oplus x_{q-1,t}. \end{cases} \qquad (3)$$

Реализация системы (3) позволяет одновременно получить q-й блок ПСП, состоящий из τ элементов. Выразим правые части системы (3) через заданные начальные условия и представим ее как систему τ булевых функций (БФ)(4) от τ переменных:

$$F(\mathbf{X}_{q-1})=\begin{cases} f_{q,\tau-1}(\mathbf{X}_{q-1})=x_{q-1,\tau-1}\oplus x_{q-1,\tau+t-1},\\ f_{q,\tau-2}(\mathbf{X}_{q-1})=x_{q-1,\tau-2}\oplus x_{q-1,\tau+t-2},\\ \dots\dots\dots\dots\dots\dots\dots\dots\\ f_{q,0}(\mathbf{X}_{q-1})=x_{q-1,0}\oplus x_{q-1,t},\end{cases}\qquad(4)$$

где $\mathbf{X}_{q-1}=[x_{q-1,0}\ \ \dots\ \ x_{q-1,\tau-2}\ \ x_{q-1,\tau-1}]$ - вектор начальных условий.

Используем правило представления БФ f_j ЛЧП (Малюгин, В.Д. Параллельные логические вычисления посредством арифметических полиномов [Текст] / В.Д. Малюгин. - М.: Наука. Физматлит, 1997. - 190 с.):

$$f_j(x_1,x_2,\dots,x_n)=\bigoplus_{i=1}^{n}a_ix_i\rightarrow L_j(x_1,x_2,\dots,x_n)=\sum_{i=1}^{n}a_ix_i,$$

где результат вычисления БФ $f_j(x_1, \dots, x_n)$ соответствует значению младшего разряда двоичного представления результата вычисления $L_j(x_1, \dots, x_n)$.

Получим систему ЛЧП:

$$\begin{cases} L_{q,\tau-1}(\mathbf{X}_{q-1})=x_{q-1,\tau-1}+x_{q-1,\tau+t-1},\\ L_{q,\tau-2}(\mathbf{X}_{q-1})=x_{q-1,\tau-2}+x_{q-1,\tau+t-2},\\ \dots\dots\dots\dots\dots\dots\dots\dots\\ L_{q,0}(\mathbf{X}_{q-1})=x_{q-1,0}+x_{q-1,t}.\end{cases}$$

Получим общий ЛЧП:

$$\begin{aligned}L(\mathbf{X}_{q-1})&=L_{q,\tau-1}(\mathbf{X}_{q-1})+2^{\gamma_1}L_{q,\tau-2}(\mathbf{X}_{q-1})+\dots+2^{\gamma_{\tau-1}}L_{q,0}(\mathbf{X}_{q-1})=\\ &=x_{q-1,\tau-1}+x_{q-1,\tau+t-1}+2^{\gamma_1}(x_{q-1,\tau-2}+x_{q-1,\tau+t-2})+\dots\\ &\dots+2^{\gamma_{\tau-1}}(x_{q-1,0}+x_{q-1,t})=h_1x_{q-1,0}+h_2x_{q-1,1}+\dots+h_\tau x_{q-1,\tau-1},\end{aligned}$$

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

$$U=L(\mathbf{X}_{q-1})=\sum_{i=1}^{\tau}h_ix_{q-1,i-1}.\quad(5)$$

Окончательный результат образуется путем реализации оператора маскирования $\Xi_t^\tau\{U\}$. Оператор маскирования $\Xi_t^\tau\{U\}$ служит для определения значения t-й БФ представления, $U=(a_\tau\dots a_t\dots a_2a_1)_2$ (запись $(\dots)_2$ означает запись в 2-ичной системе счисления), то есть $\Xi_t^\tau\{U\}=a_t$ (Шмерко, В.П. Теоремы Малюгина: новое понимание в логическом управлении, проектировании СБИС и структурах данных для новых технологий [Текст] / В.П. Шмерко // Автоматика и телемеханика. - 2004. - №6. - С. 104-112). Граф вычисления ЛЧП (5) представлен на фиг. 6.

Таким образом, полученный ЛЧП (5) позволяет реализовать q-й блок ПСП длины τ. Значения полученного блока ПСП будут являться начальным заполнением для ЛЧП, реализующего следующий блок последовательности длиной, равной τ.

Пример 1. На фиг. 7 представлен 22-разрядный ЛРРС, структура которого определяется образующим триномом $D(\chi)=\chi^{22}+\chi+1$ и характеристическим уравнением $x_{22}=x_0\oplus x_1$. Система уравнений участка ПСП длины $\tau=22$ имеет вид:

$$\left\{\begin{array}{l} x_{q,0}=x_{q-1,0}\oplus x_{q-1,1},\\ x_{q,1}=x_{q-1,1}\oplus x_{q-1,2},\\ x_{q,2}=x_{q-1,2}\oplus x_{q-1,3},\\ x_{q,3}=x_{q-1,3}\oplus x_{q-1,4},\\ x_{q,4}=x_{q-1,4}\oplus x_{q-1,5},\\ x_{q,5}=x_{q-1,5}\oplus x_{q-1,6},\\ x_{q,6}=x_{q-1,6}\oplus x_{q-1,7},\\ x_{q,7}=x_{q-1,7}\oplus x_{q-1,8},\\ x_{q,8}=x_{q-1,8}\oplus x_{q-1,9},\\ x_{q,9}=x_{q-1,9}\oplus x_{q-1,10},\\ x_{q,10}=x_{q-1,10}\oplus x_{q-1,11},\end{array}\right. \quad \left\{\begin{array}{l} x_{q,11}=x_{q-1,11}\oplus x_{q-1,12},\\ x_{q,12}=x_{q-1,12}\oplus x_{q-1,13},\\ x_{q,13}=x_{q-1,13}\oplus x_{q-1,14},\\ x_{q,14}=x_{q-1,14}\oplus x_{q-1,15},\\ x_{q,15}=x_{q-1,15}\oplus x_{q-1,16},\\ x_{q,16}=x_{q-1,16}\oplus x_{q-1,17},\\ x_{q,17}=x_{q-1,17}\oplus x_{q-1,18},\\ x_{q,18}=x_{q-1,18}\oplus x_{q-1,19},\\ x_{q,19}=x_{q-1,19}\oplus x_{q-1,20},\\ x_{q,20}=x_{q-1,20}\oplus x_{q-1,21},\\ x_{q,21}=x_{q-1,21}\oplus x_{q-1,0}\oplus x_{q-1,1}.\end{array}\right.$$

Запишем систему характеристических уравнений как систему БФ:

$$\left\{\begin{array}{l} f_{q,0}(\boldsymbol{X}_{q-1})=x_{q-1,0}\oplus x_{q-1,1},\\ f_{q,1}(\boldsymbol{X}_{q-1})=x_{q-1,1}\oplus x_{q-1,2},\\ f_{q,2}(\boldsymbol{X}_{q-1})=x_{q-1,2}\oplus x_{q-1,3},\\ f_{q,3}(\boldsymbol{X}_{q-1})=x_{q-1,3}\oplus x_{q-1,4},\\ f_{q,4}(\boldsymbol{X}_{q-1})=x_{q-1,4}\oplus x_{q-1,5},\\ f_{q,5}(\boldsymbol{X}_{q-1})=x_{q-1,5}\oplus x_{q-1,6},\\ f_{q,6}(\boldsymbol{X}_{q-1})=x_{q-1,6}\oplus x_{q-1,7},\\ f_{q,7}(\boldsymbol{X}_{q-1})=x_{q-1,7}\oplus x_{q-1,8},\\ f_{q,8}(\boldsymbol{X}_{q-1})=x_{q-1,8}\oplus x_{q-1,9},\\ f_{q,9}(\boldsymbol{X}_{q-1})=x_{q-1,9}\oplus x_{q-1,10},\\ f_{q,10}(\boldsymbol{X}_{q-1})=x_{q-1,10}\oplus x_{q-1,11},\end{array}\right. \quad \left\{\begin{array}{l} f_{q,11}(\boldsymbol{X}_{q-1})=x_{q-1,11}\oplus x_{q-1,12},\\ f_{q,12}(\boldsymbol{X}_{q-1})=x_{q-1,12}\oplus x_{q-1,13},\\ f_{q,13}(\boldsymbol{X}_{q-1})=x_{q-1,13}\oplus x_{q-1,14},\\ f_{q,14}(\boldsymbol{X}_{q-1})=x_{q-1,14}\oplus x_{q-1,15},\\ f_{q,15}(\boldsymbol{X}_{q-1})=x_{q-1,15}\oplus x_{q-1,16},\\ f_{q,16}(\boldsymbol{X}_{q-1})=x_{q-1,16}\oplus x_{q-1,17},\\ f_{q,17}(\boldsymbol{X}_{q-1})=x_{q-1,17}\oplus x_{q-1,18},\\ f_{q,18}(\boldsymbol{X}_{q-1})=x_{q-1,18}\oplus x_{q-1,19},\\ f_{q,19}(\boldsymbol{X}_{q-1})=x_{q-1,19}\oplus x_{q-1,20},\\ f_{q,20}(\boldsymbol{X}_{q-1})=x_{q-1,20}\oplus x_{q-1,21},\\ f_{q,21}(\boldsymbol{X}_{q-1})=x_{q-1,21}\oplus x_{q-1,0}\oplus x_{q-1,1}.\end{array}\right.$$

Получим систему ЛЧП:

$$\left\{\begin{array}{l} L_{q,0}(\boldsymbol{X}_{q-1}) = x_{q-1,0} + x_{q-1,1}, \\ L_{q,1}(\boldsymbol{X}_{q-1}) = x_{q-1,1} + x_{q-1,2}, \\ L_{q,2}(\boldsymbol{X}_{q-1}) = x_{q-1,2} + x_{q-1,3}, \\ L_{q,3}(\boldsymbol{X}_{q-1}) = x_{q-1,3} + x_{q-1,4}, \\ L_{q,4}(\boldsymbol{X}_{q-1}) = x_{q-1,4} + x_{q-1,5}, \\ L_{q,5}(\boldsymbol{X}_{q-1}) = x_{q-1,5} + x_{q-1,6}, \\ L_{q,6}(\boldsymbol{X}_{q-1}) = x_{q-1,6} + x_{q-1,7}, \\ L_{q,7}(\boldsymbol{X}_{q-1}) = x_{q-1,7} + x_{q-1,8}, \\ L_{q,8}(\boldsymbol{X}_{q-1}) = x_{q-1,8} + x_{q-1,9}, \\ L_{q,9}(\boldsymbol{X}_{q-1}) = x_{q-1,9} + x_{q-1,10}, \\ L_{q,10}(\boldsymbol{X}_{q-1}) = x_{q-1,10} + x_{q-1,11}, \end{array}\right. \quad \left\{\begin{array}{l} L_{q,11}(\boldsymbol{X}_{q-1}) = x_{q-1,11} + x_{q-1,12}, \\ L_{q,12}(\boldsymbol{X}_{q-1}) = x_{q-1,12} + x_{q-1,13}, \\ L_{q,13}(\boldsymbol{X}_{q-1}) = x_{q-1,13} + x_{q-1,14}, \\ L_{q,14}(\boldsymbol{X}_{q-1}) = x_{q-1,14} + x_{q-1,15}, \\ L_{q,15}(\boldsymbol{X}_{q-1}) = x_{q-1,15} + x_{q-1,16}, \\ L_{q,16}(\boldsymbol{X}_{q-1}) = x_{q-1,16} + x_{q-1,17}, \\ L_{q,17}(\boldsymbol{X}_{q-1}) = x_{q-1,17} + x_{q-1,18}, \\ L_{q,18}(\boldsymbol{X}_{q-1}) = x_{q-1,18} + x_{q-1,19}, \\ L_{q,19}(\boldsymbol{X}_{q-1}) = x_{q-1,19} + x_{q-1,20}, \\ L_{q,20}(\boldsymbol{X}_{q-1}) = x_{q-1,20} + x_{q-1,21}, \\ L_{q,21}(\boldsymbol{X}_{q-1}) = x_{q-1,21} + x_{q-1,0} + x_{q-1,1}. \end{array}\right.$$

Получим общий ЛЧП:

$$\begin{aligned} U = L(\boldsymbol{X}_{q-1}) = {} & (4 \cdot 10^{10} + 1)_{16} x_{q-1,0} + (4 \cdot 10^{10} + 5)_{16} x_{q-1,1} + \\ & + (14)_{16} x_{q-1.2} + (50)_{16} x_{q-1,3} + (140)_{16} x_{q-1,4} + (5 \cdot 10^2)_{16} x_{q-1,5} + \\ & + (14 \cdot 10^2)_{16} x_{q-1,6} + (5 \cdot 10^3)_{16} x_{q-1,7} + (14 \cdot 10^3)_{16} x_{q-1,8} + \\ & + (5 \cdot 10^4)_{16} x_{q-1,9} + (14 \cdot 10^4)_{16} x_{q-1,10} + (5 \cdot 10^5)_{16} x_{q-1,11} + \\ & + (14 \cdot 10^5)_{16} x_{q-1,12} + (5 \cdot 10^6)_{16} x_{q-1,13} + (14 \cdot 10^6)_{16} x_{q-1,14} + \\ & + (5 \cdot 10^7)_{16} x_{q-1,15} + (14 \cdot 10^7)_{16} x_{q-1,16} + (5 \cdot 10^8)_{16} x_{q-1.17} + \\ & + (14 \cdot 10^8)_{16} x_{q-1,18} + (5 \cdot 10^9)_{16} x_{q-1,19} + (14 \cdot 10^9)_{16} x_{q-1,20} + \\ & + (5 \cdot 10^{10})_{16} x_{q-1,21}, \end{aligned}$$

где запись $(\ldots)_{16}$ означает запись в 16-ричной системе счисления.

Пусть $x_{q-1,0}=1$, $x_{q-1,1}=0$, $x_{q-1,2}=0$, $x_{q-1,3}=0$, $x_{q-1,4}=0$, $x_{q-1,5}=1$, $x_{q-1,6}=0$, $x_{q-1,7}=0$, $x_{q-1,8}=0$, $x_{q-1,9}=0$, $x_{q-1,10}=0$, $x_{q-1,11}=0$, $x_{q-1,12}=1$, $x_{q-1,13}=0$, $x_{q-1,14}=0$, $x_{q-1,15}=0$, $x_{q-1,16}=1$, $x_{q-1,17}=0$, $x_{q-1,18}=0$, $x_{q-1,19}=0$, $x_{q-1,20}$, $x_{q-1,21}=1$, тогда

$$U = L(\boldsymbol{X}_{q-1}) = (4\cdot 10^{10}+1)_{16}\cdot 1 + (4\cdot 10^{10}+5)_{16}\cdot 0 + (14)_{16}\cdot 0 +$$
$$+ (50)_{16}\cdot 0 + (140)_{16}\cdot 0 + (5\cdot 10^{2})_{16}\cdot 1 + (14\cdot 10^{2})_{16}\cdot 0 +$$
$$+ (5\cdot 10^{3})_{16}\cdot 0 + (14\cdot 10^{3})_{16}\cdot 0 + (5\cdot 10^{4})_{16}\cdot 0 +$$
$$+ (14\cdot 10^{4})_{16}\cdot 0 + (5\cdot 10^{5})_{16}\cdot 0 + (14\cdot 10^{5})_{16}\cdot 1 +$$
$$+ (5\cdot 10^{6})_{16}\cdot 0 + (14\cdot 10^{6})_{16}\cdot 0 + (5\cdot 10^{7})_{16}\cdot 0 +$$
$$+ (14\cdot 10^{7})_{16}\cdot 1 + (5\cdot 10^{8})_{16}\cdot 0 + (14\cdot 10^{8})_{16}\cdot 0 +$$
$$+ (5\cdot 10^{9})_{16}\cdot 0 + (14\cdot 10^{9})_{16}\cdot 0 + (5\cdot 10^{10})_{16}\cdot 1 =$$
$$= (90141400501)_{16} =$$

$$= (\underbrace{1\ 0}_{\downarrow\, f_{q,21}}\underbrace{0\ 1}_{\downarrow\, f_{q,20}}\underbrace{0\ 0}_{\downarrow\, f_{q,19}}\underbrace{0\ 0}_{\downarrow\, f_{q,18}}\underbrace{0\ 0}_{\downarrow\, f_{q,17}}\underbrace{0\ 1}_{\downarrow\, f_{q,16}}\underbrace{0\ 1}_{\downarrow\, f_{q,15}}\underbrace{0\ 0}_{\downarrow\, f_{q,14}}\underbrace{0\ 0}_{\downarrow\, f_{q,13}}\underbrace{0\ 1}_{\downarrow\, f_{q,12}}\underbrace{0\ 1}_{\downarrow\, f_{q,11}}$$
$$\underbrace{0\ 0}_{\downarrow\, f_{q,10}}\underbrace{0\ 0}_{\downarrow\, f_{q,9}}\underbrace{0\ 0}_{\downarrow\, f_{q,8}}\underbrace{0\ 0}_{\downarrow\, f_{q,7}}\underbrace{0\ 0}_{\downarrow\, f_{q,6}}\underbrace{0\ 1}_{\downarrow\, f_{q,5}}\underbrace{0\ 1}_{\downarrow\, f_{q,4}}\underbrace{0\ 0}_{\downarrow\, f_{q,3}}\underbrace{0\ 0}_{\downarrow\, f_{q,2}}\underbrace{0\ 0}_{\downarrow\, f_{q,1}}\underbrace{0\ 1}_{\downarrow\, f_{q,0}})_2.$$

Таким образом, посредством одного ЛЧП получим g-блок ПСП длины τ=22.

В модулярной арифметике (МА) целое неотрицательное число А может быть однозначно представлено набором остатков по основаниям МА $p_1<p_2<\ldots<p_\eta<p_{\eta+1}<\ldots<p_k$:

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_\eta, \alpha_{\eta+1}, \ldots, \alpha_\kappa)_{MA}, \qquad (6)$$

где $P_\eta=p_1p_2\ldots p_\eta>A$; $\alpha_j = |A|_{p_j}$; $|\cdot|_p$ - наименьший неотрицательный вычет числа · по модулю p; $p_1<p_2<\ldots<p_\eta<p_{\eta+1}<\ldots<p_\kappa$ - попарно простые; j=1, 2, …, η, η+1, …, κ (Акушский, И.Я. Машинная арифметика в остаточных классах [Текст] / И.Я. Акушский, Д.И. Юдицкий. - М.: Советское радио, 1968. - 440 с.).

При этом остатки МА α_1, α_2, …, … α_η считаются информационными, а $\alpha_{\eta+1}$, …, α_κ - контрольными (избыточными). Сама МА является в этом случае расширенной, где $P_\kappa = P_\eta p_{\eta+1}\ldots p_\kappa$, и охватывает полное множество состояний, представляемых всеми к вычетами. Эта область будет являться полным диапазоном МА [0, P_κ) и состоять из рабочего диапазона [0, P_η), где $P_\eta=p_1p_2\ldots p_\eta$, определяемого неизбыточными основаниями МА, и диапазона, определяемого избыточными основаниями [P_η, P_κ), представляющего недопустимую область. Это означает, что операции над числом А выполняются в диапазоне [0, P_κ). Поэтому, если результат операции МА выходит за пределы P_η, то делается вывод об ошибке вычислений. Полученные числа, меньшие P_η, будем называть правильными, равные или большие P_η - неправильными (Акушский, И.Я. Машинная арифметика в остаточных классах [Текст] / И.Я. Акушский, Д.И. Юдицкий. - М.: Советское радио, 1968. - 440 с.).

Для осуществления контроля ошибок арифметических вычислений при реализации ЛЧП (5) рассмотрим систему, заданную основаниями p_1, p_2, …, p_η, …, p_κ. Представим каждый коэффициент h_i ЛЧП (5) в виде (6), построим систему малоразмерных ЛЧП вида:

$$\begin{cases} u^{(1)} = L^{(1)}(\mathbf{X}_{q-1}) = \alpha_1^{(1)} x_{q-1,0} + \ldots + \alpha_\tau^{(1)} x_{q-1,\tau-1}, \\ u^{(2)} = L^{(2)}(\mathbf{X}_{q-1}) = \alpha_1^{(2)} x_{q-1,0} + \ldots + \alpha_\tau^{(2)} x_{q-1,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u^{(\eta)} = L^{(\eta)}(\mathbf{X}_{q-1}) = \alpha_1^{(\eta)} x_{q-1,0} + \ldots + \alpha_\tau^{(\eta)} x_{q-1,\tau-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u^{(\kappa)} = L^{(\kappa)}(\mathbf{X}_{q-1}) = \alpha_1^{(\kappa)} x_{q-1,0} + \ldots + \alpha_\tau^{(\kappa)} x_{q-1,\tau-1}. \end{cases} \qquad (7)$$

Малоразмерность ЛЧП системы (7) будет обеспечиваться малой величиной коэффициентов $\alpha_1^{(1)}, \ldots, \alpha_\tau^{(1)}, \ldots, \alpha_1^{(\eta)}, \ldots, \alpha_\tau^{(\eta)}, \ldots, \alpha_1^{(\kappa)}, \ldots, \alpha_\tau^{(\kappa)}$, определяемых выбранными основаниями системы $p_1, \ldots, p_\eta, \ldots, p_\kappa$.

Подставив в (7) значения остатков системы по соответствующим основаниям для каждого коэффициента h_i ЛЧП (5), а также значения переменных $x_{q-1,0}, \ldots, x_{q-1,\tau-1}$, получим избыточный модулярный код (МК), представленный системой ЛЧП (7):

$(u^{(1)}, u^{(2)}, \ldots, u^{(\eta)}, \ldots, u^{(\kappa)})_{МК}$,

где $u^{(1)}, u^{(2)}, \ldots, u^{(\eta)}, \ldots, u^{(\kappa)}$ - целые числа.

Решим систему выражений с одним неизвестным:

$$\begin{cases} U = |u^{(1)}|_{p_1}, \\ U = |u^{(2)}|_{p_2}, \\ \ldots\ldots\ldots\ldots \\ U = |u^{(\eta)}|_{p_\eta}, \\ \ldots\ldots\ldots\ldots \\ U = |u^{(\kappa)}|_{p_\kappa}. \end{cases} \qquad (8)$$

Так как основания $p_1, p_2, \ldots, p_\eta, \ldots, p_\kappa$ попарно просты, то в соответствии с известными положениями теории чисел единственным решением системы (8) является выражение:

$$U = \left| \sum_{s=1}^{\kappa} P_{s,\kappa} \mu_{s,\kappa} u^{(s)} \right|_{P_\kappa}, \qquad (9)$$

где $P_{s,\kappa} = \dfrac{P_\kappa}{p_s} \mu_{s,\kappa} = |P_{s,\kappa}^{-1}|_{p_s}$, $P_\kappa = \prod_{s=1}^{\kappa} p_s$.

Вхождение результата вычисления (9) в рабочий диапазон (контрольное выражение):

$$0 \le U < P_\eta, \qquad (10)$$

означает отсутствие обнаруживаемых ошибок вычислений.

Пример 2. Пусть q-й блок участка ПСП представлен одним ЛЧП вида:

$L(X_{q-1})=65x_{q-1,0}+69x_{q-1,1}+20x_{q-1,2}+80x_{q-1,3}$.

Выберем основания системы: $p_1=2$, $p_2=3$, $p_3=5$, $p_4=11$, $p_5=13$, где p_5 - контрольное основание.

Рабочий и полный диапазоны системы в этом случае равны: $P_4=p_1p_2p_3p_4=330$ и $P_5=P_4p_5=4290$ соответственно.

Представим каждый коэффициент ЛЧП в виде набора остатков по выбранным основаниям системы:

$h_1=65=(1, 2, 0, 10, 0)_{MA}$,

$h_2=69=(1, 0, 4, 3, 4)_{MA}$,

$h_3=20=(0, 2, 0, 9, 7)_{MA}$,

$h_4=80=(0, 2, 0, 3, 2)_{MA}$.

Построим систему (7):

$$\begin{cases} u^{(1)} = L^{(1)}(x_{q-1,0}, x_{q-1,1}) = x_{q-1,0} + x_{q-1,1}, \\ u^{(2)} = L^{(2)}(x_{q-1,0}, x_{q-1,2}, x_{q-1,3}) = 2x_{q-1,0} + 2x_{q-1,2} + 2x_{q-1,3}, \\ u^{(3)} = L^{(3)}(x_{q-1,1}) = 4x_{q-1,1}, \\ u^{(4)} = L^{(4)}(x_{q-1,0}, \ldots, x_{q-1,3}) = 10x_{q-1,0} + 3x_{q-1,1} + 9x_{q-1,2} + 3x_{q-1,3}, \\ u^{(5)} = L^{(5)}(x_{q-1,1}, \ldots, x_{q-1,3}) = 4x_{q-1,1} + 7x_{q-1,2} + 2x_{q-1,3}. \end{cases}$$

Пусть $x_{q-1,0}=x_{q-1,1}=x_{q-1,3}=1$, $x_{q-1,2}=0$, тогда $u^{(1)}=2$, $u^{(2)}=4$, $u^{(3)}=4$, $u^{(4)}=16$, $u^{(5)}=6$, получим избыточный МК: $(2, 4, 4, 16, 6)_{MK}$.

Решим систему (8):

$$\begin{cases} U = |2|_2, \\ U = |4|_3, \\ U = |4|_5, \\ U = |16|_{11}, \\ U = |6|_{13}, \end{cases}$$

в соответствии с (9) получим: $U=214$.

Так как результат вычисления U удовлетворяет $0 \le U < 330$, то будем считать, что при вычислениях ошибка допущена не была либо произошла необнаруживаемая ошибка.

На чертежах представлено:

на фиг. 1 изображен самопроверяемый специализированный вычислитель систем булевых функций;

на фиг. 2 изображен общий вид ЛРРС;

на фиг. 3 изображена структурная схема информационных связей рекурсии (1);

на фиг. 4 изображен общий вид ЛРРС (частный случай: образующий полином - трином);

на фиг. 5 изображена структурная схема информационных связей рекурсии (2);

на фиг. 6 изображена структурная схема информационных связей ЛЧП (5);

на фиг. 7 изображена структурная схема 22-х разрядного ЛРРС.

Предлагаемое устройство содержит: шину 10 подачи значений τ булевых переменных $x_{q-1,0}$, $x_{q-1,0}$, …, $x_{q-1,\tau-1}$, шину 11 подачи коэффициентов h_1, …, h_τ ЛЧП, шину 12 подачи оснований системы (информационные: p_1, …, p_η; контрольные: $p_{\eta+1}$, …, p_κ), регистр памяти 1, блок памяти 2 коэффициентов h_1, …, h_τ ЛЧП, блоки 3.1.1, …, 3.1.τ, …, 3.η.1, …, 3.η.τ, …, 3.κ.1, …, 3.κ.τ вычисления наименьших неотрицательных вычетов числа (коэффициентов ЛЧП) по основаниям системы, множители 4.1.1, …, 4.1.τ, …, 4.η.1, …, 4.η.τ, …, 4.κ.1, …, 4.κ.τ, блок памяти 5 оснований p_1, …, p_η, $p_{\eta+1}$, …, p_κ системы, многоместные сумматоры 6.1, …, 6.η, …, 6.κ, блок 7 решения системы сравнений с одним неизвестным, блок сравнения 8, блок оператора маскирования 9, выходы 13.1, …, 13.τ выдачи значений τ БФ $f_{q,0}(X_{q-1})$, …, $f_{q,\tau-1}(X_{q-1})$ соответственно.

Шина 10 подачи значений τ булевых переменных $x_{q-1,0}$, $x_{q-1,1}$, …, $X_{q-1,\tau-1}$ является входом регистра памяти 1, шина 11 подачи коэффициентов ЛЧП является входом блока памяти 2 коэффициентов h_1, …, h_τ ЛЧП, предназначенного для их хранения, шина 12 подачи оснований системы является входом блока памяти 5 оснований p_1, …, p_η, $p_{\eta+1}$, …, p_κ системы, предназначенного для их хранения, выходы блоков памяти 2 и 5 являются входами блоков 3.1.1, …, 3.1.τ, …, 3.η.1, …, 3.η.τ, …, 3.κ.1, …, 3.κ.τ вычисления наименьших неотрицательных вычетов числа (коэффициентов ЛЧП) по соответствующим основаниям системы, выходы которых вместе с выходами регистра памяти 1 являются входами множителей 4.1.1, …, 4.1.τ, …, 4.η.1, …, 4.η.τ, …, 4.κ.1, …, 4.κ.τ, выходы которых являются входами многоместных сумматоров 6.1, …, 6.η, …, 6.κ, выходы которых являются входами блока 7 решения системы сравнений с одним неизвестным, выход которого подключен к входам блока сравнения 8 и блока оператора маскирования 9, выход блока сравнения 8 является вторым входом блока оператора маскирования 9, выходы которого являются выходами устройства выдачи значений τ БФ $f_{q,0}(X_{q-1})$, …, $f_{q,\tau-1}(X_{q-1})$ соответственно.

Предлагаемое устройство работает следующим образом.

В исходном состоянии в блоки 2 и 5 памяти занесены по шинам 11 и 12 коэффициенты h_1, …, h_τ ЛЧП и основания p_1, …, p_η, $p_{\eta+1}$, …, p_k системы соответственно, с их выходов на входы блоков 3.1.1, …, 3.1.τ, …, 3.η.1, …, 3.η.τ, …, 3.κ.1, …, 3.κ.τ вычисления наименьших неотрицательных вычетов числа (коэффициентов ЛЧП) по основаниям системы поступают коэффициенты ЛЧП (5) и основания системы. В момент времени, соответствующий началу преобразований, на входы регистра памяти 1 из шины 10 поступают значения булевых переменных $x_{q-1,0}$, $x_{q-1,1}$, …, $X_{q-1,\tau-1}$. С выходов регистра памяти 1 и блоков 3.1.1, …, 3.1.τ, …, 3.η.1, …, 3.η.τ, …, 3.κ.1, …, 3.κ.τ вычисления наименьших неотрицательных вычетов числа (коэффициентов ЛЧП) по основаниям системы на входы множителей 4.1.1, …, 4.1.τ, …, 4.η.1, …, 4.η.τ, …, 4.κ.1, …, 4.κ.τ поступают наименьшие неотрицательные вычеты $\alpha_1^{(1)},\ldots,\alpha_\tau^{(1)},\ldots,\alpha_1^{(\eta)},\ldots,\alpha_\tau^{(\eta)},\ldots,\alpha_1^{(\kappa)},\ldots,\alpha_\tau^{(\kappa)}$ и значения булевых переменных $x_{q-1,0}$, $x_{q-1,1}$, …, $X_{q-1,\tau-1}$. С выходов множителей 4.1.1, …, 4.1.τ, …, 4.η.1, …, 4.η.τ, …, 4.κ.1, …, 4.κ.τ на входы многоместных сумматоров 6.1, …, 6.η, …, 6.κ поступают произведения

$$\alpha_1^{(1)}\cdot x_{q-1,0},\ldots,\alpha_\tau^{(1)}\cdot x_{q-1,\tau-1},\ldots,\alpha_1^{(\eta)}\cdot x_{q-1,0},\ldots,\alpha_\tau^{(\eta)}\cdot x_{q-1,\tau-1},\ldots,\alpha_1^{(\kappa)}\cdot x_{q-1,0},\ldots,\alpha_\tau^{(\kappa)}\cdot x_{q-1,\tau-1}$$

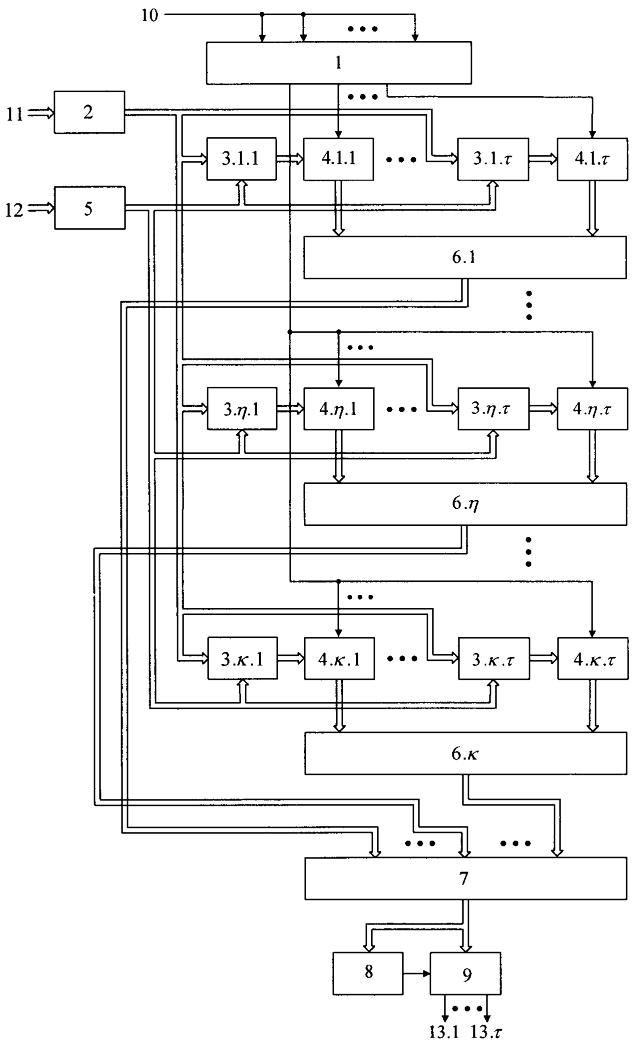
. С выходов многоместных сумматоров 6.1, …, 6.η, …, 6.κ на входы блока 7 решения системы сравнений с одним неизвестным поступают числовые результаты вычисления

ЛЧП $u^{(1)}, \ldots, u^{(\eta)}, \ldots, u^{(\kappa)}$. Значения $u^{(1)}, \ldots, u^{(\eta)}, \ldots, u^{(\kappa)}$ являются избыточным МК, представленным системой ЛЧП (7): $(u^{(1)}, u^{(2)}, \ldots, u^{(\eta)}, u^{(\eta+1)})_{МК}$, где $u^{(1)}, \ldots, u^{(\eta)}, \ldots, u^{(\kappa)}$ - целые числа. С выхода блока 7 решения системы сравнений с одним неизвестным на входы блока сравнения 8 и блока оператора маскирования 9 поступает числовой результат вычисления (9). Вхождение результата вычисления (9) в рабочий диапазон (контрольное выражение): $0 \leq U < P_\eta$ означает отсутствие обнаруживаемых ошибок вычислений. Таким образом, при отсутствии ошибок вычислений с блока сравнения 8 на вход блока оператора маскирования 9 поступает сигнал, разрешающий выполнять операцию маскирования, в противном случае - запрещающий. С выхода блока оператора маскирования 9 получим значения БФ $f_{q,0}(X_{q-1}), \ldots, f_{q,\tau-1}(X_{q-1})$, которые соответствуют элементам g-го блока ПСП $x_{q,0}, x_{q,1}, \ldots, x_{q,\tau-1}$.

Формула изобретения

Самопроверяемый специализированный вычислитель систем булевых функций, содержащий шину подачи τ булевых переменных, блок памяти, предназначенный для хранения коэффициентов линейного числового полинома, к входу которого подключена шина подачи коэффициентов; отличающийся тем, что введены регистр памяти, входы которого являются входами устройства, к которым подключена шина подачи τ булевых переменных; блок памяти, предназначенный для хранения оснований системы, к входу которого подключена шина подачи оснований системы, выходы которого вместе с выходами блока памяти хранения коэффициентов линейного числового полинома подключены к входам блоков вычисления наименьших неотрицательных вычетов числа (коэффициентов линейного числового полинома) по основаниям системы, выходы которых вместе с выходами регистра памяти подключены к входам множителей, выходы которых подключены к входам многоместных сумматоров, выходы которых подключены к входам блока решения системы сравнений с одним неизвестным, выход которого подключен к входам блока сравнения и блока оператора маскирования, выход блока сравнения подключен ко второму входу блока оператора маскирования, выходы которого являются выходами устройства выдачи значений τ булевых функций.

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ
ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ



Фиг. 1

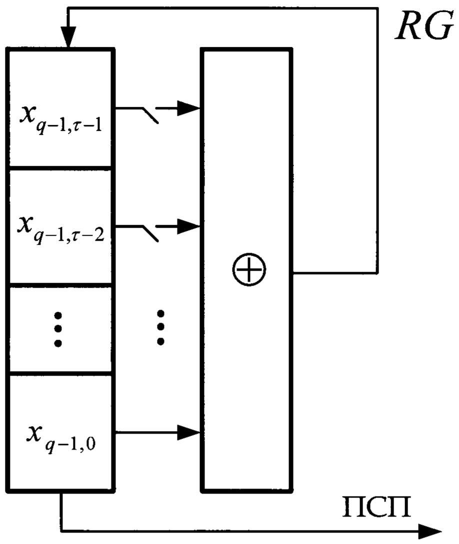
Самопроверяемый специализированный вычислитель систем булевых функций

Авторы изобретения:

С.А.Диченко
А.В.Крупенин
О.А.Финько
Д.В.Самойленко
И.В.Чечин
К.С.Меретуков
В.М.Самус

1

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ

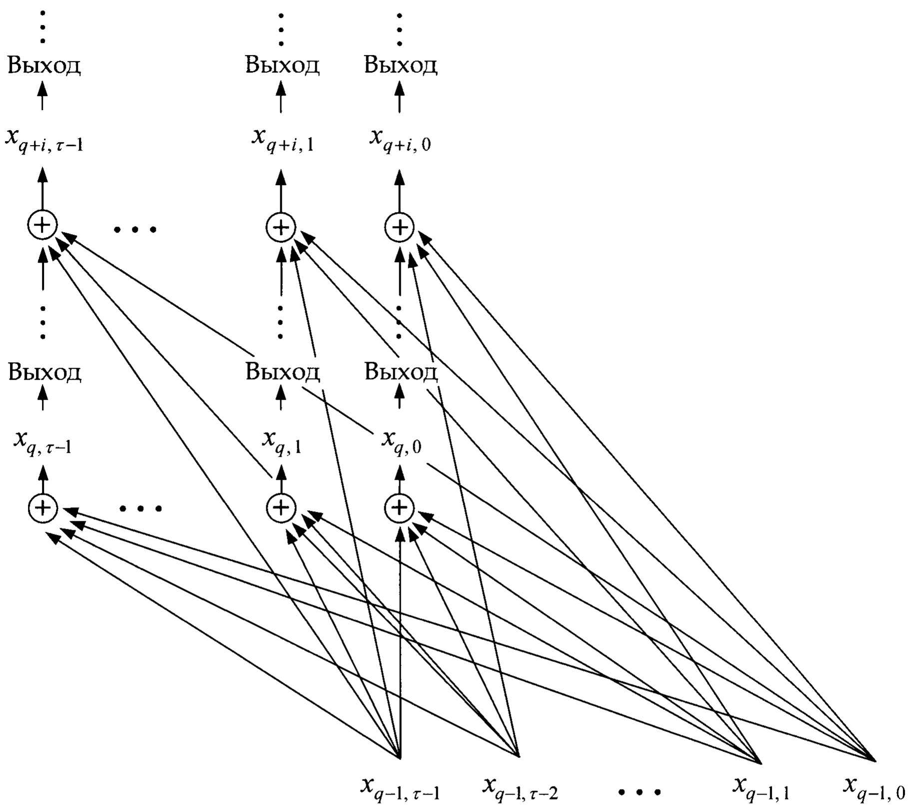


Фиг. 2
Общий вид ЛРРС
Авторы изобретения:

С.А.Диченко
А.В.Крупенин
О.А.Финько
Д.В.Самойленко
И.В.Чечин
К.С.Меретуков
В.М.Самус

2

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ



Фиг. 3

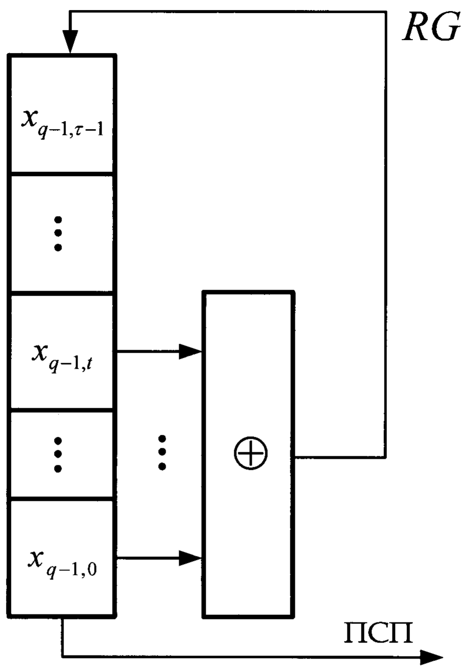
Структурная схема информационных связей рекурсии (1)

Авторы изобретения:

С.А.Диченко
А.В.Крупенин
О.А.Финько
Д.В.Самойленко
И.В.Чечин
К.С.Меретуков
В.М.Самус

3

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ
ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ

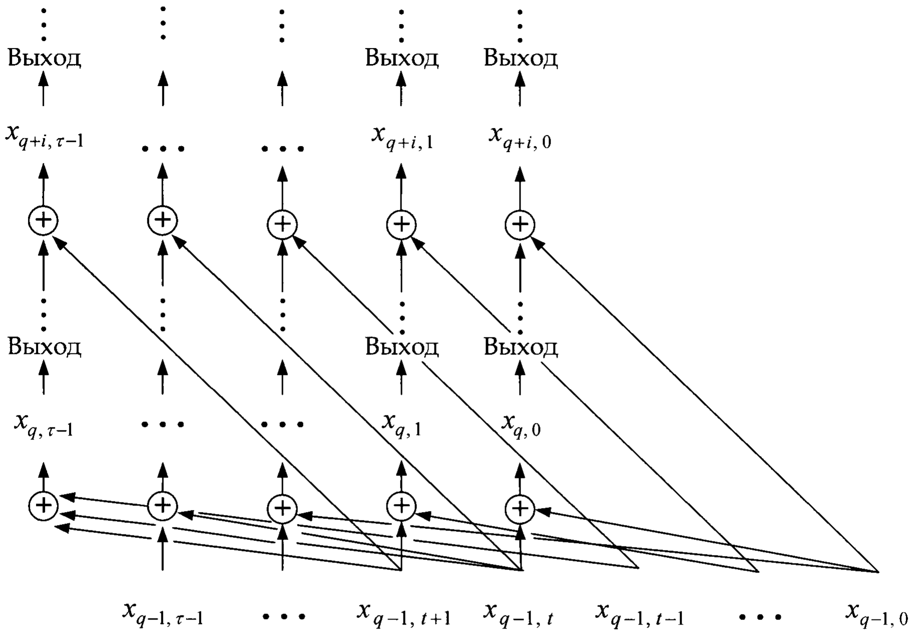


Фиг. 4
Общий вид ЛРРС (частный случай: образующий полином – трином)

Авторы изобретения:

С.А.Диченко
А.В.Крупенин
О.А.Финько
Д.В.Самойленко
И.В.Чечин
К.С.Меретуков
В.М.Самус

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ



Фиг. 5

Структурная схема информационных связей рекурсии (2)

Авторы изобретения:

С.А.Диченко

А.В.Крупенин

О.А.Финько

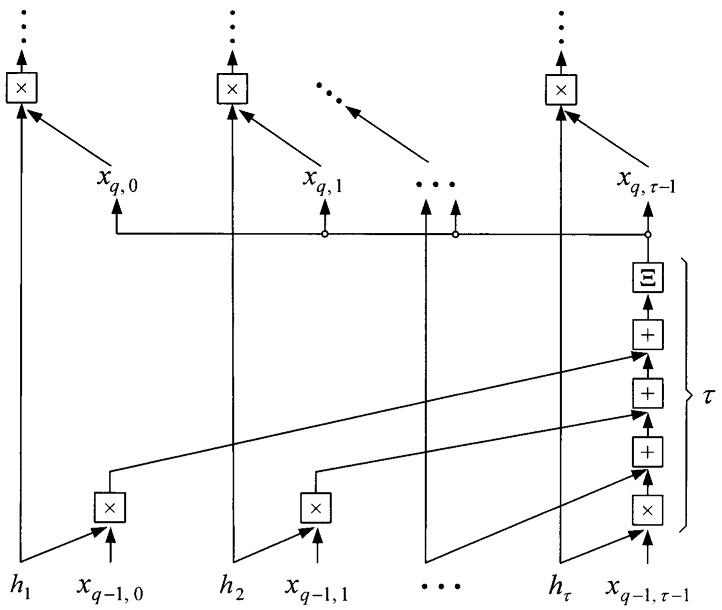
Д.В.Самойленко

И.В.Чечин

К.С.Меретуков

В.М.Самус

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ
ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ

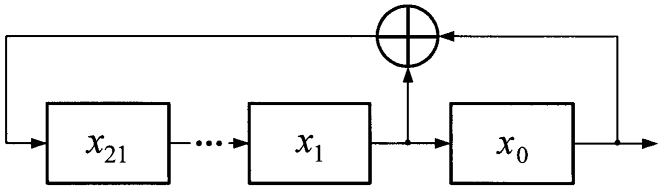


Фиг. 6
Структурная схема информационных связей ЛЧП (5)
Авторы изобретения:

С.А.Диченко
А.В.Крупенин
О.А.Финько
Д.В.Самойленко
И.В.Чечин
К.С.Меретуков
В.М.Самус

6

САМОПРОВЕРЯЕМЫЙ СПЕЦИАЛИЗИРОВАННЫЙ ВЫЧИСЛИТЕЛЬ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ



Фиг. 7

Структурная схема 22-х разрядного ЛРРС

Авторы изобретения:

С.А.Диченко
А.В.Крупенин
О.А.Финько
Д.В.Самойленко
И.В.Чечин
К.С.Меретуков
В.М.Самус