РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 776 346**(13) **C1**

(51) МПК
G06F 7/58 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 7/58 (2021.08)

(21)(22) Заявка: **2021120045, 08.07.2021**

(24) Дата начала отсчета срока действия патента:
08.07.2021

Дата регистрации:
19.07.2022

Приоритет(ы):
(22) Дата подачи заявки: **08.07.2021**

(45) Опубликовано: **19.07.2022** Бюл. № **20**

Адрес для переписки:
115409, Москва, Каширское ш., 31, НИЯУ МИФИ ОУИС УНИ Бейгул Г.В.

(72) Автор(ы):
Иванов Михаил Александрович (RU),
Саликов Евгений Александрович (RU),
Козлов Александр Александрович (RU),
Григорьев Михаил Павлович (RU),
Хисамутдинов Марат Айдарович (RU),
Чуркин Кирилл Юрьевич (RU)

(73) Патентообладатель(и):
федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский ядерный университет МИФИ" (НИЯУ МИФИ) (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2740339 C1, 13.01.2021. US 8433740 B2, 30.04.2013. US 6044388 A, 28.03.2000. US 20050044119 A1, 24.02.2005. EP 2000901 B1, 10.12.2008. JP 6900176 B2, 15.06.2017.**

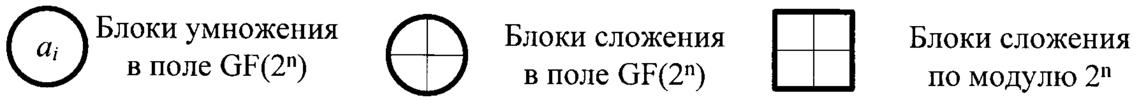
(54) ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

(57) Реферат:

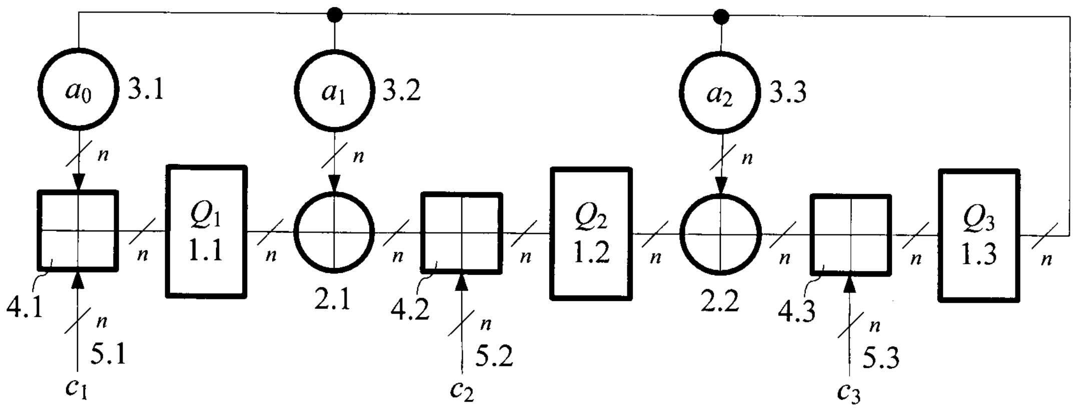
Настоящее изобретение относится к области вычислительной техники для защиты информации. Технический результат заключается в упрощении устройства генератора псевдослучайных чисел и увеличении длины формируемой псевдослучайной последовательности. Технический результат достигается за счёт N регистров 1.1, 1.2, …, 1.N разрядности n, (N-1) блоков 2.1, 2.2, …, 2.(N-1) сложения в $GF(2^n)$, N блоков 3.1, 3.2, …, 3.N умножения в $GF(2^n)$, причем величина, на которую происходит умножение в (i+1)-м блоке умножения, равна коэффициенту a_i характеристического многочлена $\phi(x)=(x+1)\lambda(x)=x^N+a_{N-1}x^{N-1}+\ldots+a_2x^2+a_1x+a_0$, а также N сумматоров 4.1, 4.2, …, 4.N по модулю 2^n. 8 ил.

RU 2776346 C1

RU 2776346 C1



GF(2^n), $\varphi(x) = x^3 + a_2x^2 + a_1x + a_0x$



$$Q_1^* = Q_3 \boxplus c_1$$
$$Q_2^* = Q_1 \oplus a_1Q_3 \boxplus c_2$$
$$Q_3^* = Q_2 \oplus a_2Q_3 \boxplus c_3$$

Фиг. 1

RU 2776346 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 776 346**(13) **C1**

(51) Int. Cl.
G06F 7/58 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 7/58 (2021.08)

(21)(22) Application: **2021120045, 08.07.2021**

(24) Effective date for property rights:
08.07.2021

Registration date:
19.07.2022

Priority:
(22) Date of filing: **08.07.2021**

(45) Date of publication: **19.07.2022** Bull. № **20**

Mail address:
115409, Moskva, Kashirskoe sh., 31, NIYAU MIFI OUIS UNI Bejgul G.V.

(72) Inventor(s):
Ivanov Mikhail Aleksandrovich (RU),
Salikov Evgenij Aleksandrovich (RU),
Kozlov Aleksandr Aleksandrovich (RU),
Grigorev Mikhail Pavlovich (RU),
Khisamutdinov Marat Ajdarovich (RU),
Churkin Kirill Yurevich (RU)

(73) Proprietor(s):
federalnoe gosudarstvennoe avtonomnoe obrazovatelnoe uchrezhdenie vysshego obrazovaniya "Natsionalnyj issledovatelskij yadernyj universitet MIFI" (NIYAU MIFI) (RU)

(54) PSEUDORANDOM NUMBER GENERATOR

(57) Abstract:

FIELD: computer technology.

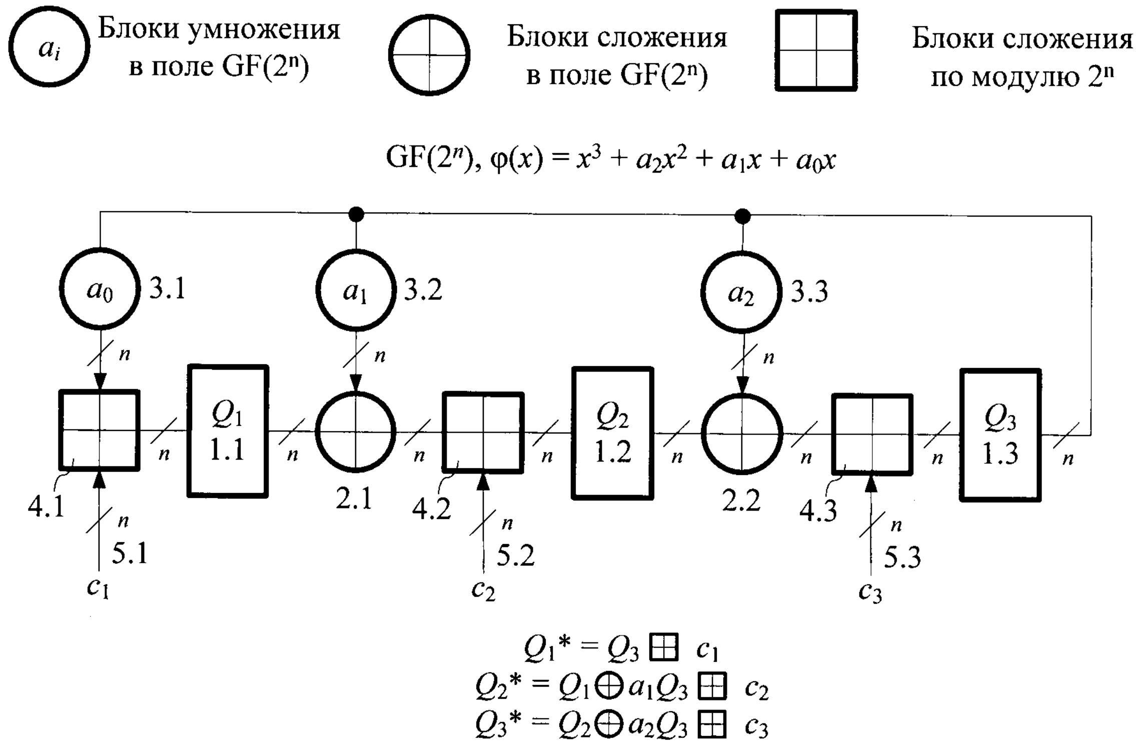
SUBSTANCE: present invention relates to the field of computer technology for information protection. The expected result is achieved due to N registers 1.1, 1.2, …, 1.N with n bits capacity, (N-1) blocks 2.1, 2.2, ..., 2.(N-1) for addition in GF(2^n), N blocks 3.1, 3.2, ..., 3.N for multiplication in GF(2^n), and the value by which multiplication occurs in the (i+1)-st multiplication block is equal to the coefficient a_i of the characteristic polynomial $\varphi(x)=(x+1)\lambda(x)=x^N+a_{N-1}x^{N-1}+\ldots+a_2x^2+a_1x+a_0$, as well as N adders 4.1, 4.2, …, 4.N, modulo 2^n.

EFFECT: simplifying the design of the pseudorandom number generator and increasing the length of the generated pseudorandom sequence.

1 cl, 8 dwg

RU 2776346 C1

RU 2776346 C1



Фиг. 1

RU 2776346 C1

Изобретение относится к вычислительной технике и электросвязи, предназначено для решения задач защиты компьютерной информации. Наиболее предпочтительной областью использования изобретения является реализация стохастических методов защиты информации.

В совокупности признаков заявленного изобретения используются следующие термины:

Регистры сдвига с линейной обратной связью (LFSR - Linear Feedback Shift Register) - простейшие генераторы псевдослучайных чисел (ГПСЧ), активно используемые при решении различных задач защиты информации. Структура устройства определяется видом двоичного характеристического многочлена Φ(x) (см. [Стохастические методы и средства защиты информации в компьютерных системах и сетях / М.А. Иванов, А.В. Ковалев, И.В. Чугунков и др. - М.: КУДИЦ-ПРЕСС, 2009, 602 с.] или [Иванов М.А., Чугунков И.В. Криптографические методы защиты информации. - М.: НИЯУ МИФИ, 2012, www.aha.ru/~msa]).

Конечное поле или поле Галуа GF(q) (GF - Galois Field, $q=p^n$ - число элементов поля, p - простое, n - натуральное) - конечное множество элементов, обладающее следующими свойствами: 1) в поле определены две операции, одна условно называется сложением, другая - умножением; 2) для элементов поля α, β, γ справедливы соотношения $\alpha+\beta=\beta+\alpha$, $\alpha\beta=\beta\alpha$, $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$; 3) в поле существуют нулевой и единичный элементы, обозначаемые соответственно как 0 и 1, для которых справедливо $0+\alpha=\alpha$, $0\alpha=0$, $1\alpha=\alpha$; 4) в поле для любого $\alpha\neq0$ существует обратный ему элемент по сложению, обозначаемый $(-\alpha)$, для которого справедливо $\alpha+(-\alpha)=0$; и обратный ему элемент по умножению, обозначаемый α^{-1}, для которого справедливо $\alpha\alpha^{-1}=1$; 5) любой ненулевой элемент поля можно представить в виде степени примитивного элемента ω: $\forall\alpha\neq0\ \alpha=\omega^i$, таким образом, конечное поле можно представить в виде $GF(q)=\{0, \omega^0=1, \omega, \omega^2, \ldots, \omega^{q-2}\}$.

Генераторы псевдослучайных чисел (ГПСЧ) - основа стохастических методов защиты информации, применение ГПСЧ обеспечивает непредсказуемое поведение объекта и средств его защиты, позволяя тем самым защититься от активного противника.

Последовательности, формируемые генераторами на основе регистров сдвига с линейными обратными связями - LFSR (Linear Feedback Shift Register), функционирующих в конечных полях, являются важнейшим классом псевдослучайных последовательностей (ПСП). Основными достоинствами этих генераторов являются:

- простота программной и аппаратной реализации; удобство интегрального исполнения из-за регулярной структуры, максимальное быстродействие;

- гарантированно большой период и хорошие статистические свойства формируемых ПСП;

- возможность построения на их основе генераторов, обладающих свойствами, ценными при решении специфических задач защиты информации (формирование последовательностей произвольной длины, формирование последовательностей с предпериодом, формирование ПСП с произвольным законом распределения, построение генераторов, обладающих свойством самоконтроля, и т.п.).

Математический аппарат, лежащий в основе LFSR, - теория конечных полей или полей Галуа. Существует две конструкции LFSR - схема Фибоначчи и схема Галуа, при этом вторая конструкция имеет много интересных свойств, которые используются и в заявленном техническом решении.

LFSR, к сожалению, не являются непредсказуемыми, поэтому применяются при решении задач криптографической защиты информации лишь в качестве строительных блоков.

Исходная информация для построения двоичного LFSR - так называемый характеристический многочлен. Степень этого многочлена определяет разрядность регистра сдвига, а ненулевые коэффициенты - характер обратных связей.

Известен генератор псевдослучайных чисел, функционирующий в конечном поле GF(p), где p>2 - простое, состоящий из N регистров разрядности $]\log_2 p[$, N блоков сложения в GF(p), N блоков умножения в GF(p), причем величина, на которую происходит умножение в (i+1)-м блоке умножения, равна коэффициенту a_i характеристического многочлена $\phi(x)=(x-1)\lambda(x)=x^N-a_{N-1}x^{N-1}-\ldots-a_2x^2-a_1x-a_0$, где i=0, 1, 2, …, (N-1), $a_i \in GF(p)$, $\lambda(x)$ - многочлен степени (N-1), примитивный над GF(p), выходы N-го регистра соединены со входами всех блоков умножения, выходы j-х блоков умножения соединены с первыми входами j-х блоков сложения, выходы которых соединены со входами j-х регистров, где j=1, 2, …, N, вторые входы всех блоков сложения образуют N групп управляющих входов генератора, выходы k-х регистров соединены со третьими входами (k+1)-х блоков сложения, выходы которых соединены со входами (j+1)-х регистров, где k=1, 2, (N-1). (M.A. Ivanov, B.V. Kliuchnikova, E.A. Salikov, A.V. Starikovskii. New class of non-binary pseudorandom number generators. - Proceedings of Intelligent Technologies in Robotics, Moscow, Russia, 2019, pp. 255-262).

Недостатком известного генератора является сложность и зависимость длины формируемой последовательности от числа элементов поля, так как число запрещенных состояний устройства равно p.

Таким образом, наиболее близким по своей технической сущности к заявленному устройству является генератор псевдослучайных чисел, функционирующий в конечном поле $GF(2^n)$, где n>1 - целое, состоящий из N регистров разрядности n, N блоков сложения в $GF(2^n)$, блока управляющих воздействий и N блоков умножения в $GF(2^n)$, причем величина, на которую происходит умножение в (i+1)-м блоке умножения, равна коэффициенту a_i характеристического многочлена $\phi(:c)=(x+1)\lambda(x)$ $=x^N+a^{N-1}+\ldots+a_2x^2+a_1x+a_0$, где i=0, 1, 2, …, (N-1), $a_i \in GF(2^n)$, $\lambda(x)$ - многочлен степени (N-1), примитивный над $GF(2^n)$, Выходы N-го регистра соединены со входами всех блоков умножения, выходы (j+1)-х блоков умножения и выходы j-х регистров соединены соответственно с первыми и вторыми входами j-х блоков сложения, выходы которых соединены со входами (j+1)-х регистров, где j=1, 2, (N-1), первые входы N-го блока сложения в $GF(2^n)$ подключены к выходам первого блока умножения, а выходы соединены со входами первого регистра, вторые входы N-го блока сложения и третьи входы j-х блоков сложения подключены к соответствующим выходам блока управляющих воздействий [Иванов М.А., Саликов Е.А. Генератор псевдослучайных чисел. Патент РФ №2740339].

Известное устройство функционирует в конечном поле $GF(2^n)$ и формирует последовательность длиной $2^{nN}-2^n+1$. Недостатком известного устройства является избыточная сложность из-за наличия блока управляющих воздействий, формирующего последовательности управляющих сигналов.

Техническим результатом изобретения является упрощение устройства и увеличение длины формируемой псевдослучайной последовательности.

Поставленная цель достигается тем, что генератор псевдослучайных чисел, функционирующий в конечном поле $GF(2^n)$, где $n>1$ - целое, состоящий из N регистров разрядности n, (N-1) блоков сложения в $GF(2^n)$, N блоков умножения в $GF(2^n)$, причем величина, на которую происходит умножение в (i+1)-м блоке умножения, равна коэффициенту a_i характеристического многочлена

$$\phi(x)=(x+1)\lambda(x)=x^N+a_{N-1}x^{N-1}+\ldots+a_2x^2+a_1x+a_0,$$

где $i=0, 1, 2, \ldots, (N-1)$, $a_i \in GF(2^n)$, $\lambda(x)$ - многочлен степени (N-1), примитивный над $GF(2^n)$, выходы N-го регистра соединены со входами всех блоков умножения, выходы (j+1)-х блоков умножения и выходы j-х регистров, где j=1, 2, (N-1), соединены соответственно с первыми и вторыми входами j-х блоков сложения, дополнительно содержит N сумматоров по модулю 2^n, выходы (i+1)-х сумматоров по модулю 2^n подключены ко входам (i+1)-х регистров, первые и вторые входы (i+1)-х сумматоров по модулю 2^n подключены к выходам (i+1)-х блоков умножения и (i+1)-м группам управляющих входов генератора.

Заявленный эффект обеспечивается за счет того, что из схемы ГПСЧ исключается блок управляющих воздействий, так как все управляющие сигналы - это константы, а диаграмма переключений генератора включает в себя два цикла длиной 2^{nN} - 2 и 2, т.е. длина формируемой последовательности не зависит от числа элементов поля.

На фиг. 1 показана схема генератора для случая $GF(2^n)$, N=3, где 1.1, 1.2, 1.3 - регистры генератора Q_1, Q_2, Q_3; 2.1, 2.2 - блоки сложения в $GF(2^n)$; 3.1, 3.2 - блоки умножения в $GF(2^n)$, причем величина, на которую происходит умножение, определяется соответствующим коэффициентом характеристического многочлена; 4.1, 4.2, 4.3 - сумматоры по модулю 2^n; 5.1, 5.2, 5.3 - группы управляющих входов генераторы, соответственно c_1, c_2, c_3.

Генератор псевдослучайных чисел, в общем случае состоит из N регистров 1.1, 1.2, …, 1.N разрядности n, (N-1) блоков 2.1, 2.2, 2.(N-1) сложения в $GF(2^n)$, N блоков 3.1, 3.2, 3.N умножения в $GF(2^n)$, причем величина, на которую происходит умножение в (i+1) -м блоке умножения, равна коэффициенту а, характеристического многочлена

$$\phi(x)=(x+1)\lambda(x)=x^N+a_{N-1}x^{N-1}+\ldots+a_2x^2+a_1x+a_0,$$

где $i=0, 1, 2, \ldots, (N-1)$, $a_i \in GF(2^n)$, $\lambda(x)$ - многочлен степени (N-1), примитивный над $GF(2^n)$, выходы N-го регистра 1.N соединены со входами всех блоков 3 умножения, выходы (j+1)-х блоков 3 умножения и выходы j-х регистров 1, где j=1, 2, …, (N-1), соединены соответственно с первыми и вторыми входами j-х блоков 2 сложения. Генератор содержит также N сумматоров 4.1, 4.2, …, 4.N по модулю 2^n, выходы (i+1)-х сумматоров 4 по модулю 2^n подключены ко входам (i+1)-х регистров 1, первые и вторые входы (i+1)-х сумматоров 4 по модулю 2п подключены к выходам (i+1)-х блоков 3 умножения и (i+1)-м группам управляющих входов 5 генератора.

Если какой-либо коэффициент $a_1, a_2, \ldots, a_{N-1}$ характеристического многочлена равен 1, это эквивалентно умножению на 1 в соответствующем блоке 3 умножения, иначе говоря, его отсутствию. Если какой-либо коэффициент $a_1, a_2, \ldots, a_{N-1}$ характеристического многочлена равен 0, это эквивалентно отсутствию соответствующих блока 2 сложения и блока 3 умножения. Таким образом, число блоков 3 умножения равно числу не равных нулю или единице коэффициентов характеристического многочлена (на фиг. 2 и 5 это число равно двум). Если какой-либо управляющий сигнал c_1, c_2, …, c_N равен 0, это эквивалентно отсутствию соответствующего сумматора 4 по модулю 2^n. Таким образом, число сумматоров 4 по модулю 2^n равно числу не равных нулю управляющих сигналов 5 (на фиг. 2 и 5 это число равно единице).

На фиг. 2 показан первый пример генератора для случая поля $GF(2^2)$, когда характеристический многочлен степени N=3 имеет вид $(x+1)(x^2+x+\omega)=x^3+\omega^2x+\omega$, где $x^2+x+\omega$ - многочлен, примитивный над $GF(2^2)$. На фиг. 3 показано соответствие между различными формами представления элементов поля $GF(2^2)$. На фиг. 4 показана диаграмма переключений генератора, схема которого приведена на фиг. 2.

На фиг. 5 показан второй пример генератора для случая поля $GF(2^3)$, когда характеристический многочлен степени N=3 имеет вид $(x+1)(x+\omega)=x^2+\omega^3x+\omega$, где $x+\omega$ - многочлен, примитивный над $GF(2^3)$. На фиг. 6 показано соответствие между различными формами представления элементов поля $GF(2^3)$. На фиг. 7 показана диаграмма переключений генератора, схема которого приведена на фиг. 5.

На фиг. 8 показан третий пример генератора для случая поля $GF(2^2)$, когда характеристический многочлен степени N=2 имеет вид $(x+1)(x+\omega)=x^2+\omega^2x+\omega$, где $x+\omega$ - многочлен, примитивный над $GF(2^2)$. На фиг. 8 показаны также две диаграммы переключений вида 14-2 генератора для разных значений управляющих сигналов c_1, c_2.

Генератор псевдослучайных чисел (ГПСЧ) работает следующим образом. Перед началом работы регистры 1 генератора устанавливаются в одно из состояний цикла длиной 2^{nN}-2. Два состояния, входящие в цикл длиной 2, являются запрещенными. Цепь установки в исходное состояние на фиг. 1 не показана. Тактовые входы регистров 1 объединены и образуют тактовый вход ГПСЧ, который также не показан на фиг. 1.

При поступлении тактовых импульсов ГПСЧ переключается в соответствии с уравнениями, приведенными на фиг. 1. Вне зависимости от используемого конечного поля $GF(2^n)$ диаграмма переключений генератора всегда имеет вид $(2^{nN}-2)$-2, т.е. состоит из двух циклов длиной 2^{nN}-2 и 2. Выходная псевдослучайная последовательность длиной 2^{nN}-2 считывается с выходов одного из регистров 1 генератора. В примерах ГПСЧ, приведенных на фиг. 4 и 7 диаграммы переключений имеют вид 62-2. В примерах ГПСЧ, приведенных на фиг. 8, диаграммы переключений имеют вид 14-2. ГПСЧ, схема которого приведена на фиг. 2, формирует псевдослучайную последовательность длиной 62 над $GF(2^2)$; ГПСЧ, схема которого приведена на фиг. 5, формирует псевдослучайную последова-тельность длиной 62 над $GF(2^3)$; ГПСЧ, схема которого приведена на фиг. 8, формирует псевдослучайные последовательности длиной 14 над $GF(2^2)$.

Таким образом, техническим результатом изобретения является упрощение устройства и увеличение длины формируемой последовательности.

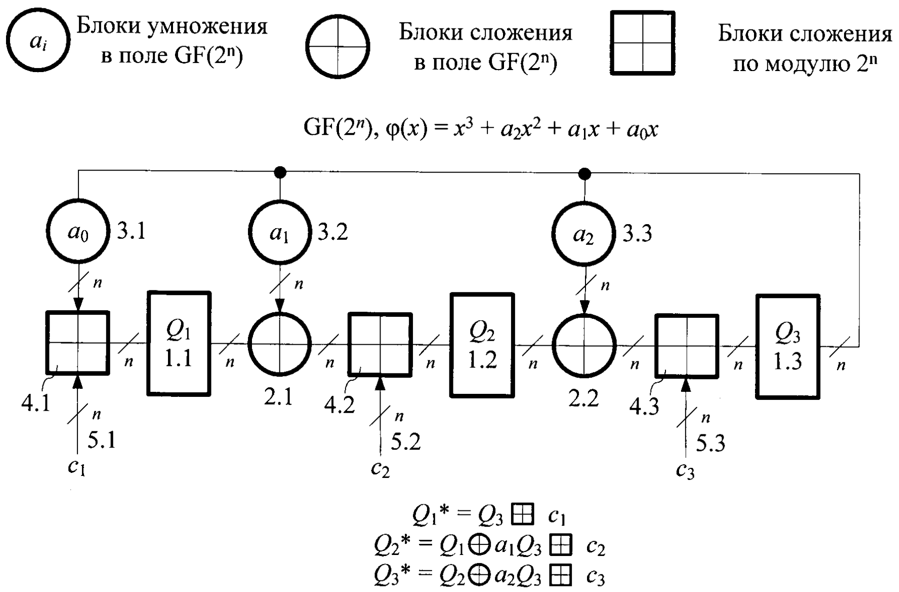
В устройстве-прототипе требуется дополнительная логика для реализации блока управляющих сигналов, которые меняются в процессе работы устройства. Число запрещенных состояний в устройстве-прототипе растет с ростом n и равно 2^n, в предлагаемом же изобретении число запрещенных состояний не зависит от n и всегда равно двум. Значения управляющих сигналов не меняются в процессе работы устройства и поэтому никакой дополнительной логики не требуется.

В устройстве-прототипе длина формируемой последовательности зависит от n и на 2^n меньше максимально возможной длины, равной 2^{nN}, в предлагаемом же изобретении длина формируемой последовательности не зависит от n и на 2 меньше максимально возможной длины, равной 2^{nN}.

(57) Формула изобретения

Генератор псевдослучайных чисел, состоящий из N регистров разрядности n, (N-1) блоков сложения в $GF(2^n)$, N блоков умножения в $GF(2^n)$, причем величина, на которую происходит умножение в (i+1)-м блоке умножения, равна коэффициенту a_i характеристического многочлена $\phi(x)=(x+1)\lambda(x)=x^N+a_{N-1}x^{N-1}+\ldots+a^2x^2+a_1x+a_0$, где i=0, 1, 2, …, (N-1), $a_i \in GF(2^n)$, $\lambda(x)$ - многочлен степени (N-1), примитивный над $GF(2^n)$, выходы N-го регистра соединены со входами всех блоков умножения, выходы (i+1)-х блоков умножения и выходы j-х регистров, где j=1, 2, …, (N-1), соединены соответственно с первыми и вторыми входами j-х блоков сложения, отличающийся тем, что он дополнительно содержит N сумматоров по модулю 2^n, выходы (i+1)-х сумматоров по модулю 2^n подключены ко входам (i+1)-х регистров, первые и вторые входы (i+1)-х сумматоров по модулю 2^n подключены к выходам (i+1)-х блоков умножения и (i+1)-м группам управляющих входов генератора.

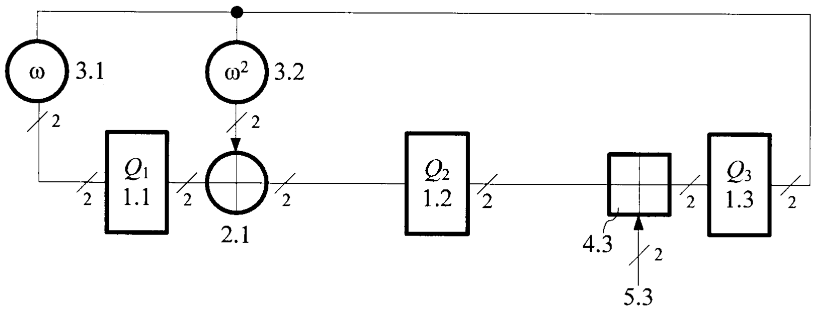
1


Блоки умножения в поле GF(2^n)
Блоки сложения в поле GF(2^n)
Блоки сложения по модулю 2^n
GF(2^n), φ(x) = x^3 + a2x^2 + a1x + a0x
a0 3.1
a1 3.2
a2 3.3
Q1 1.1
Q2 1.2
Q3 1.3
2.1
2.2
4.1
4.2
4.3
5.1
5.2
5.3
c1
c2
c3
n
Q1* = Q3 ⊞ c1
Q2* = Q1 ⊕ a1Q3 ⊞ c2
Q3* = Q2 ⊕ a2Q3 ⊞ c3

Фиг. 1

2

$\mathrm{GF}(2^2)$, $\varphi(x) = (x + 1)(x^2 + x + \omega) = x^3 + \omega^2 x + \omega$, $c_1c_2c_3 = 001$



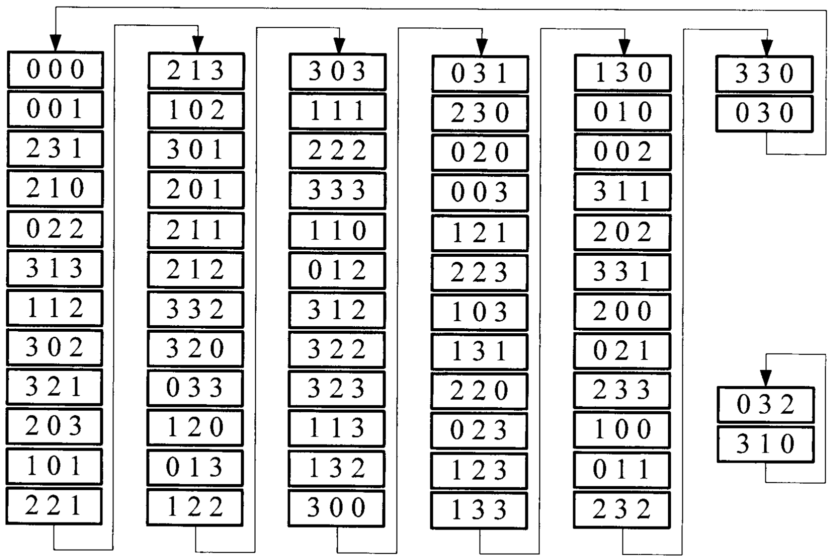
$Q_1^* = \omega Q_3$
$Q_2^* = Q_1 \oplus \omega^2 Q_3$
$Q_3^* = Q_2 \boxplus 1$

Фиг. 2

3

0	00	0	0
1	01	1	1
ω	10	2	x
ω^2	11	3	$x + 1$

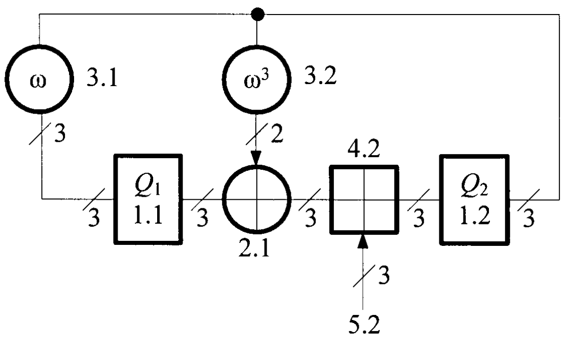
Фиг. 3



Фиг. 4

4

$GF(2^2)$, $\varphi(x) = (x + 1)(x + \omega) = x^2 + \omega^3 x + \omega$, $c_1 c_2 = 03$

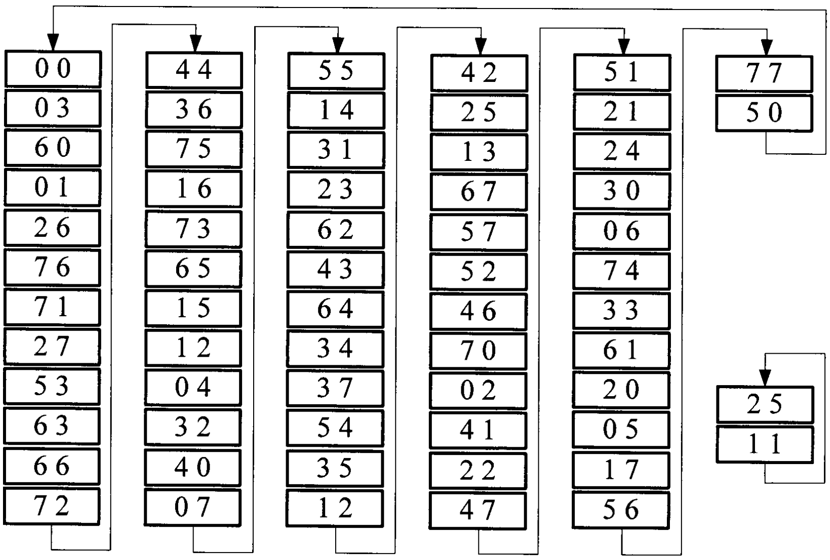


$$Q_1^* = \omega Q_2$$
$$Q_2^* = Q_1 \ominus \omega^3 Q_2 \boxplus 3$$

Фиг. 5

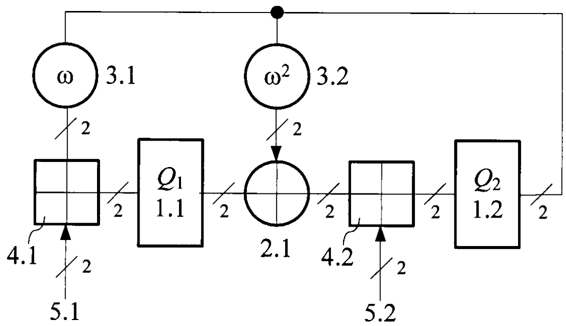
0	000	0	0
1	001	1	1
ω	010	2	x
ω^2	100	4	x^2
ω^3	011	3	$x + 1$
ω^4	110	6	$x^2 + x$
ω^5	111	7	$x^2 + x + 1$
ω^6	101	5	$x^2 + 1$

Фиг. 6

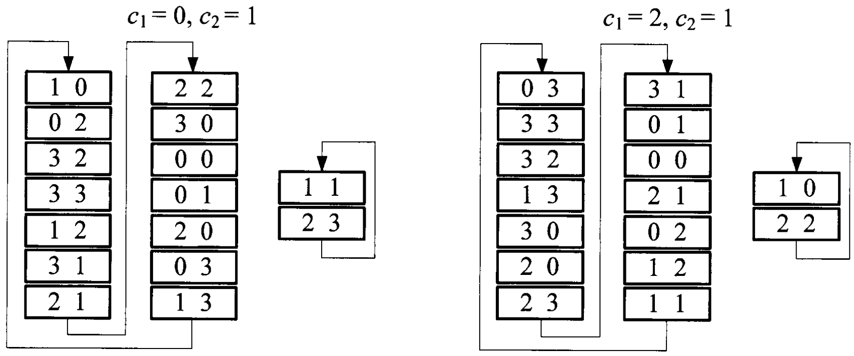


Фиг. 7

$$GF(2^2)=\{0,\ 1,\ \omega,\ \omega^2\},\ \omega^3=1,\ \omega^2+\omega+1=0;$$
$$\varphi(x)=(x+1)(x+\omega)=x^2+\omega^2x+\omega$$



$$Q_1^*=\omega Q_2 \boxplus c_1,$$
$$Q_2^*=Q_1 \oplus \omega^2 Q_2 \boxplus c_2.$$



Фиг. 8