На правах рукописи

Саликов Евгений Александрович

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА РЕГИСТРАХ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

2.3.2 – «Вычислительные системы и их элементы» (технические науки)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Автор: Саликов Евгений Александрович

Москва – 2023 г.

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Научный руководитель:
Иванов Михаил Александрович
доктор технических наук, профессор кафедры «Компьютерные системы и технологии», Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ».

Официальные оппоненты:
Грибунин Вадим Геннадьевич
доктор технических наук, доцент, главный научный сотрудник автономной некоммерческой организации «Институт инженерной физики»;

Куприянов Михаил Степанович
доктор технических наук, профессор, заведующий кафедрой вычислительной техники, Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина);

Антонов Александр Александрович
кандидат технических наук, доцент факультета программной инженерии и компьютерных техники, Федеральное Государственное Автономное Образовательное Учреждение Высшего Образования «Национальный Исследовательский Университет ИТМО».

Защита состоится 16 ноября 2023 г. в 16 час. 00 мин. на заседании диссертационного совета МИФИ.2.01 федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ» (115409, г. Москва, Каширское шоссе, 31).

С диссертацией можно ознакомиться в библиотеке и на сайте http://ds.mephi.ru федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Автореферат разослан «____» _____2023 г.

Ученый секретарь
диссертационного совета, к.т.н. Веселов Д.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Важным элементом вычислительной техники являются генераторы псевдослучайных чисел (ГПСЧ).

Как справедливо отмечается многими авторами[1], в различных отраслях науки и техники приходится сталкиваться с процессами или объектами сложной структуры, для исследования которых затруднительно эффективно применять классические аналитические методы. В этих ситуациях используется имитационное моделирование, требующее генерации случайных чисел.

Аналогичные особенности имеют место и при проведении испытаний объектов цифровой техники на надежность, живучесть и отказоустойчивость, при решении задач защиты информации от случайных и умышленных деструктивных воздействий. Непрерывный рост сложности цифровых устройств (ЦУ), повышение степени интеграции элементной базы определяют повышенные требования к обеспечению указанных характеристик. Перспективным направлением во всех этих случаях следует признать применение стохастических алгоритмов обработки данных, главный результат использования которых – внесение непредсказуемости в работу ЦУ, как в программном, так и аппаратном исполнении. Речь идет о таких универсальных приемах, как рандомизация, обфускация и полиморфизм.

ЭВМ, функционирование которых основано на использовании генераторов случайных или псевдослучайных чисел, принято называть стохастическими вычислительными машинами (СтВМ), при этом можно говорить о двух направлениях развития СтВМ:

- вычислительные машины и системы, использующие вероятностное представление информации;
- ЭВМ, в которых используется или рандомизация последовательности адресов, или рандомизация среды исполнения программ, или рандомизация архитектуры.

Задача генерации случайных чисел в компьютерных системах и сетях решается различными способами. Первый предполагает использование физических процессов различной природы, преобразуемых в цифровую форму, пригодную для обработки в ЭВМ. Основной недостаток такого подхода – это ограниченная точность формирования требуемых статистических характеристик. Кроме того, физические источники случайности подвержены влиянию дестабилизирующих факторов, отсутствует возможность повторной генерации последовательностей для подтверждения ранее полученных результатов, практически всегда при

[1] Кузнецов В.М., Песошин В.А. Генераторы случайных и псевдослучайных последовательностей на цифровых элементах задержки. – Казань, Изд-во Казан. Гос. техн. ун-та, 2013.

реализации этого подхода применяются уникальные методы схемотехнического построения, не допускающие программной реализации. Иначе говоря, случайные последовательности чрезвычайно сложно формировать, поэтому они очень часто заменяются на псевдослучайные.

Качественные псевдослучайные последовательности (ПСП), являясь детерминированными, обладают, тем не менее, почти всеми свойствами реализации истинно случайных процессов и успешно их заменяют во многих приложениях. Можно отметить такие достоинства второго подхода, основанного на использовании ПСП, как гарантированная и сколь угодно высокая точность формирования требуемых статистических характеристик, отсутствие влияния дестабилизирующих факторов, отсутствие проблем с подтверждения полученных результатов, возможность программной реализации. Самый существенный недостаток второго подхода – сложности в части обеспечения важнейшего требования по непредсказуемости формируемых последовательностей.

Стоит упомянуть и третий подход, основанный на предположении, что случайные последовательности можно получить, если инициализировать качественный ГПСЧ случайными значениями в случайные моменты времени. Иначе говоря, третий подход предполагает использование ГПСЧ совместно с внешними источниками случайности, включая физические.

Требования к качественному ГПСЧ:

- непредсказуемость;
- статистическая безопасность;
- гарантированно большой период формируемых ПСП;
- эффективная программная или аппаратная реализация.

Важнейшим классом ГПСЧ являются генераторы на регистрах сдвига с линейными и нелинейными обратными связями. Их основные достоинства:

- Хорошие статистические свойства формируемых ПСП;
- Гарантированно большой период формируемых последовательностей;
- Эффективнейшая программная и аппаратная реализация;
- Максимальное быстродействие;
- Регулярная структура, удобная для интегрального исполнения.

Развитием теории ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями в нашей стране занимались в разные годы В.Н. Ярмолик, В.А. Песошин, В.М. Кузнецов, В.И. Доценко, Р.Г. Фараджев, О.А. Козлитин, на западе – А. Гилл (A. Gill), С.В. Голомб (S.W. Golomb), Б. Элспас (B. Elspas), Е. Дуброва (E. Dubrova) и другие.

Математический аппарат, лежащий в основе ГПСЧ рассматриваемого класса – это, в первую очередь, теория конечных полей или полей Галуа GF(p^n). В этой части можно отметить фундаментальные работы Ю.Л. Сагаловича.

Области использования этих генераторов:

– Вероятностное тестирование ЦУ (Random Testing);
– Встроенное диагностирование СБИС (Built-in Self Testing);
– Кодирование с обнаружением и исправлением ошибок при передаче данных по каналам связи (Error Correcting Coding);
– Построение систем связи с шумоподобными сигналами;
– Скремблирование информации (Data Scrambling Techniques);
– Синтез синхронных счетчиков, в том числе самопроверяемых;
– Обфускация логики работы средств вычислительной техники (Design Obfuscation);
– Контроль хода выполнения программ и микропрограмм в ЭВМ (Online Checking of Control Flow);
– Реализация стохастических методов обработки информации, в том числе минималистских (Light-Weight) для RFID-систем и Интернета вещей.

В последнем случае, учитывая главный недостаток этих генераторов, связанный с предсказуемостью формируемых последовательностей, они применяются лишь в качестве строительных блоков, особенно в тех ситуациях, где к ГПСЧ предъявляются наиболее жесткие требования. Самый показательный пример на эту тему – это реализация одного из трех раундовых преобразований в специфицированном в новом российском стандарте ГОСТ Р 34.12-2015 алгоритме Кузнечик. Шаг перемешивания состояния алгоритма стохастического преобразования – суть шестнадцать тактов работы 16-разрядного генератора Фибоначчи, функционирующего в конечном поле $GF(2^8)$.

Наконец, стоит упомянуть возможность использования схем с линейными и нелинейными обратными связями на цифровых элементах задержки для реализации физически неклонируемых функций (Physical Unclonable Functions), одна из областей применения которых – защита от аппаратных закладок.

Таким образом, развитие теоретической и схемотехнической базы ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями является актуальной научной задачей.

Объектом исследования в диссертации являются стохастические алгоритмы преобразования данных.

Предметом исследования являются ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями.

Целью работы является повышение эффективности стохастических алгоритмов за счет увеличения периода формируемых последовательностей, исключения линейных зависимостей между отдельными фрагментами недвоичных ПСП, обеспечения возможности самоконтроля правильности функционирования ГПСЧ, разработки схем генераторов, ориентированных на реализацию технологий Design Obfuscation и Logic Obfuscation.

Для достижения поставленной цели в работе решались следующие **задачи**:

1) Обобщение результатов, полученных в последние годы в части двоичных ГПСЧ, функционирующих в GF(2) на случай генераторов, функционирующих в конечных полях общего вида GF(p^n); разработка математических моделей и логических схем генераторов ($M - p + 1$)-, ($M - 2^n + 1$) и ($M - 1$)-последовательностей, где p – простое, n – натуральное;
2) Разработка методов перехода от генераторов M-, ($M - p + 1$)-, ($M - 2^n + 1$) и ($M - 1$)-последовательностей к генераторам ($M + 1$)-последовательностей, т.е. генераторам ПСП максимально возможной длины при заданном количестве элементов памяти;
3) Разработка методов синтеза ГПСЧ, обладающих свойством самоконтроля, на основе выбора характеристических полиномов специального вида;
4) Разработка логических схем ГПСЧ, ориентированных на реализацию технологий Design Obfuscation и Logic Obfuscation;
5) Разработка математических и программных моделей ГПСЧ новых классов и проведение исследований их технических характеристик.

Соответствие паспорту специальности 2.3.2.

Направления исследований:

- Разработка научных основ создания новых классов ГПСЧ, исследование их свойств и принципов функционирования;
- Теоретический анализ и экспериментальное исследование функционирования генераторов на регистрах сдвига с линейными и нелинейными обратными связями с целью улучшения их технических характеристик;
- Разработка методов, алгоритмов и программ, обеспечивающих надежность, контроль и диагностирование ЦУ, учитывая возможность применения ГПСЧ рассматриваемого класса для решения задач встроенного диагностирования, контроля целостности, а самое главное – внесения непредсказуемости в работу цифровых объектов и средств обеспечения их надежности, живучести и отказоустойчивости.

Методы исследований. При проведении исследований и разработок в диссертационной работе были использованы теория линейных последовательностных машин, теория полей Галуа, а также методы стохастической информатики.

Научная новизна. В результате выполнения работы получены следующие новые научные результаты:

- Известные результаты исследований двоичных генераторов (M – 1)-последовательностей обобщены на случай генерации

($M - 2^n + 1$)- и ($M - 1$)-последовательностей, функционирующих в конечном поле GF(2^n), где $n > 1$ – целое;
- Разработаны методы построения недвоичных генераторов ($M + 1$)-последовательностей на базе ГПСЧ, функционирующих в конечном поле GF(p^n), где p – простое, n – натуральное;
- Разработаны логические схемы ГПСЧ, ориентированных на реализацию концепции Design Obfuscation и Logic Obfuscation, которые предназначены на решение задач соответственно защиты от использования технических решений по двойному назначению и защиты от реверс-инжиниринга логических схем генераторов;
- Разработаны математические модели всех разработанных ГПСЧ;
- Разработан алгоритм поиска управляющих воздействий, при подаче которых на входы ГПСЧ, функционирующих в поле GF(2^n), последние превращаются в генераторы ($M - 2^n + 1$)-последовательностей;
- Разработан новый алгоритм хеширования данных на основе использования модифицированной конструкции SPONGE и многомерных стохастических преобразований.

Практическая значимость работы.

ГПСЧ все чаще используются в тех приложениях, где требуется высокая надежность функционирования. Известные методы аппаратного контроля ЦУ в реальном масштабе времени, такие как дублирование, контроль с использованием корректирующих кодов и другие, требуют значительных аппаратных затрат на их реализацию.

Разработан метод построения недвоичных ГПСЧ в конечном поле GF(p^n) с самоконтролем правильности функционирования на основе выбора характеристических полиномов специального вида. Метод основан на предсказании значения свертки содержимого элементов памяти генератора. Одна из возможных областей применения метода – синтез синхронных самопроверяемых счетчиков.

Разработана программная модель генератора ($M - p + 1$)-последовательностей, где p – простое. Разработана программная модель генератора ($M - 2^n + 1$)-последовательностей, где n – натуральное. Разработана программная модель генератора ($M - 1$)-последовательности на основе ГПСЧ, функционирующих в поле GF(2^n).

Разработанные программные модели ориентированы на проведение экспериментальных исследований разработанных ГПСЧ и выявления их технических характеристик, в частности на определение управляющих воздействий на входы генераторов, при которых последние приобретают требуемые свойства, а также упрощения процедуры синтеза ГПСЧ с самоконтролем.

Апробация результатов. Результаты работы докладывались на всероссийской конференции The Radio-Electronic Devices and Systems for Infocommunication Technologies» (REDS-2019) и на четырех международных

конференциях Advanced Technologies in Robotics and Intelligent Systems (2020), IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2019, ElConRus 2020 и EIConRus 2022).

Публикации. По результатам работы опубликованы 15 печатных работ, в том числе 6 в печатных изданиях, индексированных в Scopus и Web of Science, а также получены четыре патента на изобретения РФ.

Внедрение. Результаты работы внедрены в учебный процесс НИЯУ МИФИ, РГУ нефти и газа (НИУ) имени И.М. Губкина и Государственного университета управления, а также в учебную и научную деятельность АНО "Центр стратегических оценок и прогнозов".

Личный вклад автора заключается в выборе направлений исследований, постановке задачи, разработке математических и программных моделей новых типов ГПСЧ, проведении исследований эксплуатационных характеристик этих устройств, разработке практических рекомендаций по их применению.

Вошедшие в диссертацию результаты получены лично автором, либо при его активном непосредственном участии. Наличие соавторов отражено в списке использованных источников информации, который включает в том числе и перечень публикаций соискателя.

Структура и объем работы. Работа состоит из введения. четырех глав, заключения, приложения, списка использованных источников информации. Она содержит 115 страниц, включая 79 рисунков, 9 таблиц, 83 наименований источников информации.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во *введении* обоснована актуальность проводимых в работе исследований, сформулированы цель и задачи диссертационной работы, научная новизна и практическая значимость полученных результатов, сформулированы основные положения, выносимые на защиту.

В *первой главе* приведена информация об областях использования ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями, их основных эксплуатационных характеристиках. Приведены требования к ГПСЧ, дана классификация ГПСЧ, при этом в качестве параметров классификации тип используемой нелинейной функции, структура ГПСЧ, тип используемых табличных преобразований, характер доступа к элементам ПСП, использование внешних параметров классификации.

Рассмотрены математические основы ГПСЧ на регистрах сдвига с линейными обратными связями, иначе говоря, ГПСЧ, функционирующих в полях Галуа. Приведена общая схема ГПСЧ, функционирующего в $GF(p^n)$, исходная информация для его построения – характеристический полином $\varphi(x)$, примитивный над $GF(p^n)$. Если степень $\varphi(x)$ равна N, тогда в состав ГПСЧ входят N регистров, N блоков умножения (БУ) в поле $GF(p^n)$, $(N-1)$-блоков сложения (БС) в поле $GF(p^n)$. С выходов любого из регистров снимается M-последовательность длиной $p^{nN}-1$. Диаграмма пере-

ключений имеет вид $(p^{nN} - 1)$-1, иначе говоря, состоит из двух кодовых колец: одно длиной $p^{nN} - 1$, включающее все ненулевые состояния генератора, другое длиной 1, включающее состояние «все нули», переходящее само в себя.

Во *второй главе* показано, как известные результаты в части генерации двоичных $(M - 1)$-последовательностей обобщаются на случай генерации p-ичных $(M - p + 1)$-последовательностей, где p – простое. Диаграмма переключений ГПСЧ в этом случае состоит из двух циклов длиной $(p^N - p)$ и p, где N – число регистров ГПСЧ, равное степени характеристического p-ичного полинома особого вида $\varphi(x) = (x - 1)\lambda(x)$, где $\lambda(x)$ – полином, примитивный над GF(p). Сумма по модулю p значений сигналов на управляющих входах генератора должна быть отлична от нуля.

Как и в двоичном случае, можно поставить задачу синтеза на основе генератора $(M - p + 1)$-последовательности, функционирующего в GF(p), генератора $(M + 1)$-последовательности.

Разработанный алгоритм построения генератора $(M + 1)$-последовательности, где $M = p^N - 1$:

- Выбор характеристического полинома степени N вида $\varphi(x) = (x - 1)\lambda(x)$, где $\lambda(x)$ – полином, примитивный над GF(p);
- Синтез генератора $(M - p + 1)$-последовательностей, соответствующего выбранному $\varphi(x)$, и построение его диаграммы переключений, которая имеет вид $(p^N - p)$-p;
- Выбор состояния Ω_1 генератора, принадлежащего кодовому кольцу длиной $p^N - p$ диаграммы переключения, из которого будет осуществляться переход в кодовое кольцо длиной p;
- Выбор состояния Ω_2 генератора, принадлежащего кодовому кольцу длиной p диаграммы переключения, из которого будет осуществляться возврат в кодовое кольцо длиной $p^N - p$;
- Синтез селектора, на выходе которого формируется сигнал $z = 1$, когда генератор оказывается в состоянии Ω_1 или в состоянии Ω_2; иначе говоря,

$$z = ((q_1 q_2 \ldots q_N) = \Omega_1) \text{ OR } ((q_1 q_2 \ldots q_N) = \Omega_2);$$

- Ввод в схему генератора блоков коррекции (БК) на элементах XOR, которые инвертируют сигналы на входах соответствующих элементов памяти генератора, обеспечивая его переход из состояния Ω_1 в малое кодовое кольцо и переход из состояния Ω_2 в большое кодовое кольцо диаграммы переключений.

На рис. 1 показан пример построения генератора пятеричной $(M + 1)$-последовательности для случая $p = 5$, $N = 2$, $\varphi(x) = (x - 1)(x + 3) = x^2 + 2x + 2$. На рис. 2 показан пример схемы селектора.

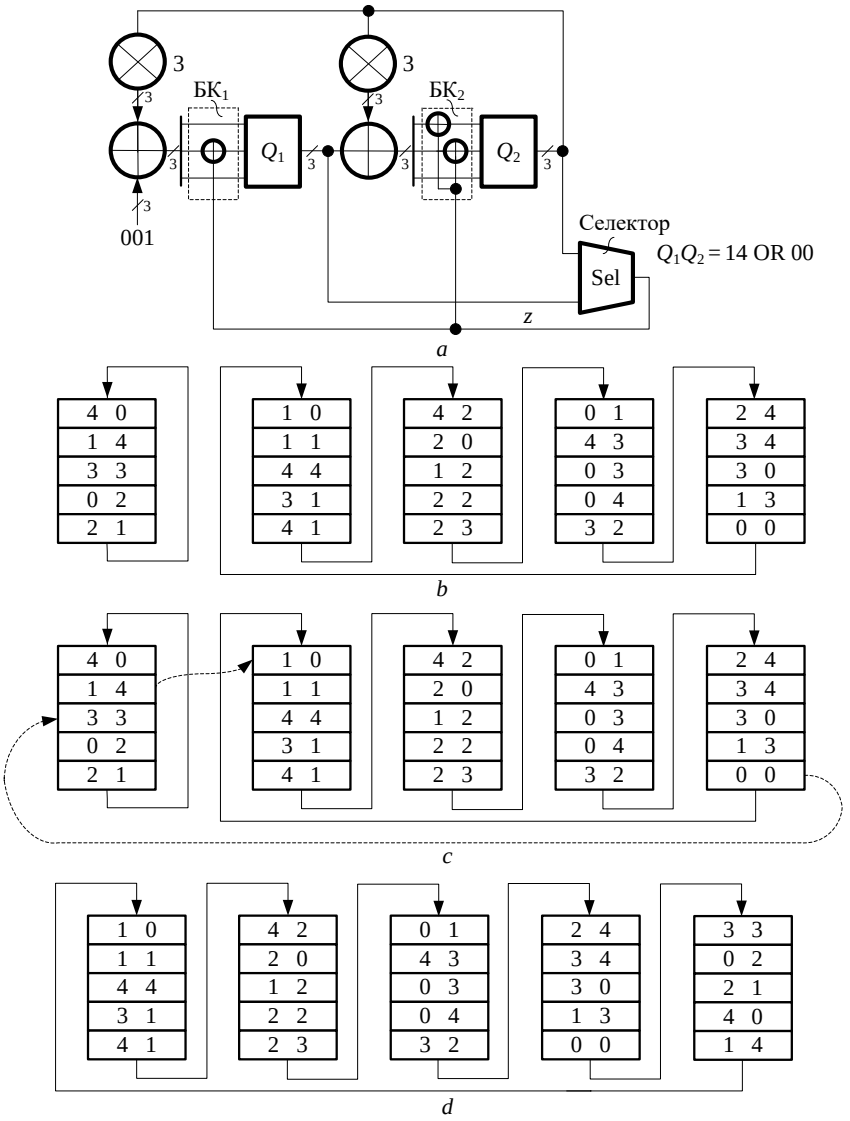


Рисунок 1 – Пример генератора пятеричной последовательности длиной 25: *a* – схема устройства;.*b* – диаграмма переключений вида 20-5 генератора-прототипа; с – идея построения генератора последовательности длиной 25, $\Omega_1 = 00$, $\Omega_2 = 14$; *d* – диаграмма переключений генератора последовательности длиной 25.

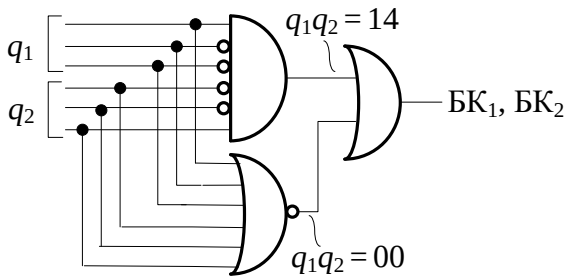


Рисунок 2.4 – Схема селектора.

Далее поставлена задача синтеза генераторов ($M – 2^n + 1$)-последовательностей для расширенных полей GF(2^n).

На рис. 3 показан пример генератора Галуа для случая $\varphi(x) = (x + 1)(x^2 + x + \omega) = x^3 + \omega^2 x + \omega$, где $\lambda(x) = x^2 + x + \omega$ – полином, примитивный над $GF(2^2) = \{0, 1, \omega, \omega^2\}$, $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$. БУ осуществляют умножение на ω, ω^2 и 0, в последнем случае это эквивалентно отсутствию соответствующего БС на схеме устройства. Диаграмма переключений генератора состоит из четырех циклов длиной 15 и четырех циклов длиной 1. При правильной работе устройства свертка Σ в поле $GF(2^2)$ состояний регистров генератора не меняет своего значения. В первом столбце диаграммы переключений $\Sigma = 1$, во втором столбце $\Sigma = \omega$, в третьем столбце $\Sigma = \omega^2$, в четвертом столбце $\Sigma = 0$, так как

$$\omega^2 + \omega + 0 = \omega^2 + \omega^2 + 1 = \omega + \omega + 1 = 1 + 1 + 1 = 0 + 0 + 1 = 1,$$
$$\omega^2 + 1 + 0 = \omega^2 + \omega^2 + \omega = \omega + \omega + \omega = 1 + 1 + \omega = 0 + 0 + \omega = \omega,$$
$$1 + \omega + 0 = \omega^2 + \omega^2 + \omega^2 = \omega + \omega + \omega^2 = 1 + 1 + \omega^2 = 0 + 0 + \omega^2 = \omega^2,$$
$$\omega^2 + \omega + 1 = \omega^2 + \omega^2 + 0 = \omega + \omega + 0 = 1 + 1 + 0 = 0 + 0 + 0 = 0.$$

Для того, чтобы построить генератор $(M – 2^n + 1)$-последовательностей в поле $GF(2^n)$, аналогичный генератору $(M – p + 1)$-последовательностей в поле $GF(p)$, необходим принципиально другой подход. Метод построения генераторов $(M – p + 1)$-последовательностей в поле $GF(p)$ в случае поля $GF(2^n)$, к сожалению, не работает.

Предложено на управляющие входы генератора подавать не фиксированные, как в известном случае, а динамически изменяющиеся значения.

Решение основано на использовании блока управляющих воздействий (БУВ). На рис. 4 показана схема устройства для случая $N = 3$, $\varphi(x) = x^3 + a_2 x^2 + a_1 x + a_0$, где $a_i \in GF(2^n)$, БС – блоки сложения в поле $GF(2^n)$, БУ – блоки умножения на a_0, a_1 и a_2 в поле $GF(2^n)$.

Важно отметить, что не на всех своих выходах БУВ формирует фиксированные значения управляющих сигналов c, как это имеет место в случае поля $GF(p)$. На некоторых выходах БУВ формируются фиксированные значения, на некоторых, периодические переменные значения. Например, в случае $GF(2^2)$, на каком-то выходе БУВ в каждом нечетном такте может формироваться одно значение, в каждом нечетном – другое; это будет обозначаться так – $1/\omega^2$, в этом случае в каждом нечетном такте на соответствующем выходе БУВ присутствует 1 (01), в каждом четном такте – ω^2 (11).

На рис. 5 показан пример предлагаемого устройства для случая $n = 2$, $\varphi(x) = (x + 1)(x^2 + x + \omega) = x^3 + \omega^2 x + \omega$, где $\lambda(x) = x^2 + x + \omega$ – полином, примитивный над $GF(2^2) = \{0, 1, \omega, \omega^2\}$, $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$. БУ осуществляют умножение соответственно на ω, ω^2 и 0 в поле $GF(2^2)$, в последнем случае это эквивалентно отсутствию соответствующего блока умножения на схеме устройства. В рассматрива-

емом случае с двух выходов БУВ поступают нули, с третьего – последовательность управляющих сигналов $\omega\ \omega^2\ \omega\ \omega^2\ \omega\ \omega^2\ \ldots$. Диаграмма переключений устройства состоит из двух циклов длиной 60 и длиной 4, как показано на рис. 6.

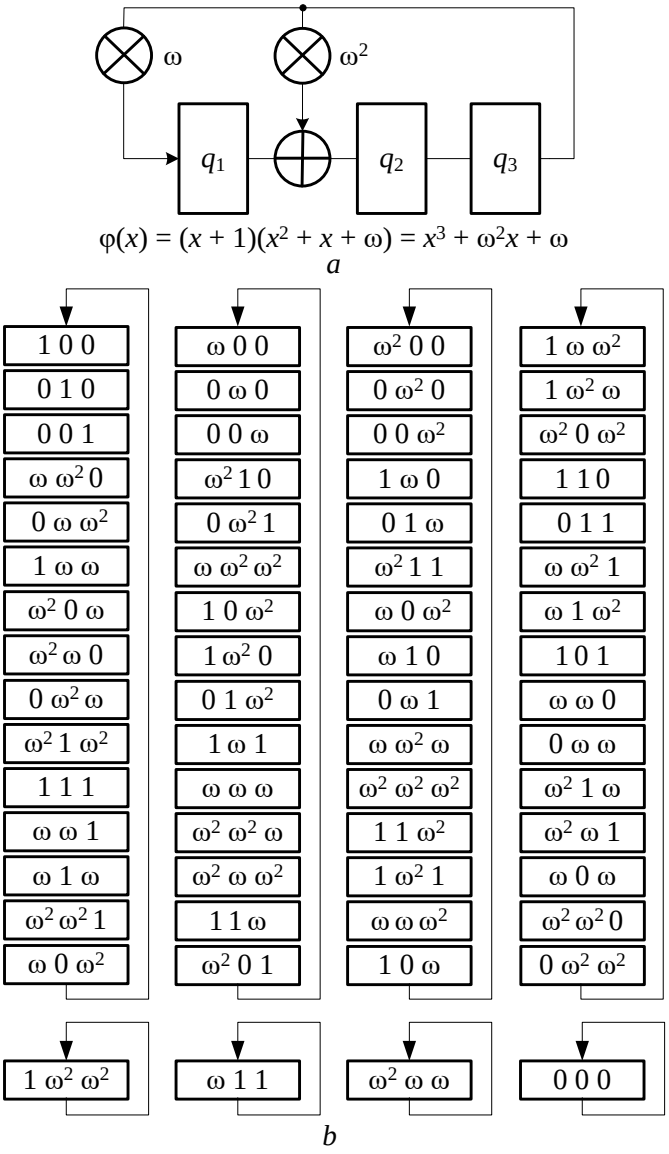


Рисунок 3 – Генератор Галуа при $\varphi(x) = (x + 1)(x^2 + x + \omega) = x^3 + \omega^2 x + \omega$, где $\lambda(x) = x^2 + x + \omega$ – полином, примитивный над $GF(2^2)$: *a* – схема устройства, *b* – диаграмма переключений.

По аналогии с известными генераторами $(M - p + 1)$-последовательностями генераторы, показанные на рис. 2 и 3 могут быть названы генератором $(M - 2^n + 1)$-последовательностей и генератором $(M - 3)$-последовательностей соответственно, где $M = 2^{nN} - 1$.

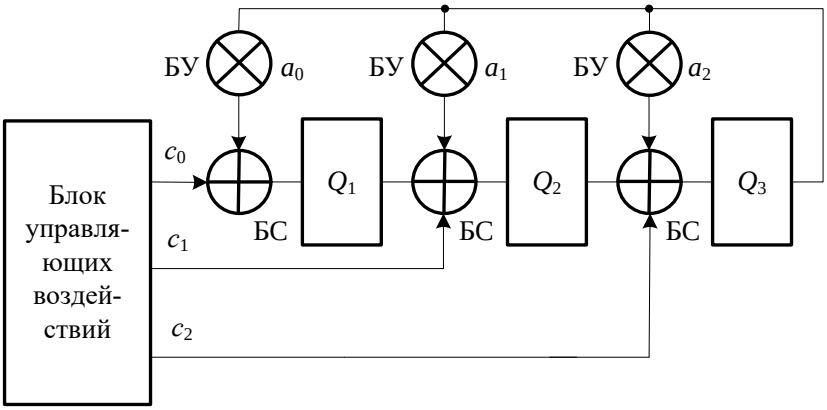


Рисунок 4 – Схема генератора (M – 2^n + 1)-последовательностей при N = 3.

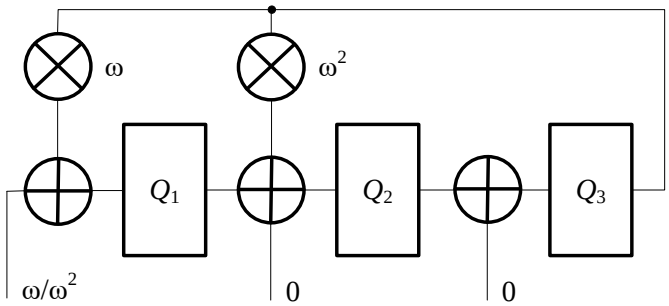


Рисунок 5 – Пример генератора (M – 3)-последовательности с диаграммой переключений 60-4 при n = 2, N = 3.

В общем случае диаграмма переключений устройства данного типа будет состоять из двух циклов длиной (M – 2^n + 1) и 2^n, где $M = 2^{nN} - 1$. При реализации технологии Design Obfuscation это позволяет реализовать 2^n скрытых функций (Hidden Functions) защищаемого устройства.

В общем случае при произвольных значениях n и N уравнения работы ГПСЧ данного типа имеют вид

$$\begin{cases} Q_1(t+1) = a_0 Q_N(t) + c_1(t), \\ Q_k(t+1) = a_{k-1} Q_N(t) + Q_{k-1}(t) + c_k(t), k = 2,3,\dots,N, \end{cases}$$

где $Q_i(t)$ и $Q_i(t+1)$ – состояния i-го регистра генератора соответственно в моменты времени t и (t + 1), $c_i(t)$ – управляющее воздействие в момент времени t, поступающее с соответствующего выхода БУВ, а все операции выполняются в поле GF(2^n).

Для случая, рассмотренного на рис. 5, уравнения принимают вид

$$\begin{cases} Q_1(t+1) = \omega Q_3(t) + \omega \text{ в каждом нечетном такте}, \\ Q_1(t+1) = \omega Q_3(t) + \omega^2 \text{ в каждом четном такте}, \\ Q_2(t+1) = \omega^2 Q_3(t) + Q_1(t), \\ Q_3(t+1) = Q_2(t). \end{cases}$$

где все операции выполняются в поле $GF(2^2) = \{0, 1, \omega, \omega^2\}$, $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$. При корректной работе генератора значение свертки содержимого всех регистров меняется по закону $0\ \omega\ 1\ \omega^2\ 0\ \omega\ 1\ \omega^2\ \ldots$.

Важно отметить, что состояния генератора, попадающие в малое кодовое кольцо диаграммы переключений, зависят от вида управляющих воздействий с выхода БУВ и от начального состояния ГПСЧ.

Рассмотрим более сложный случай. На рис. 6, *a* показан генератор (M – 2^n + 1)-последовательностей при $n = 3$, $\varphi(x) = (x + 1)(x + \omega) = x^2 + \omega^3 x + \omega$, где $\lambda(x) = x + \omega$ – полином, примитивный над $GF(2^3) = \{0, 1, \omega, \ldots, \omega^6\}$, $\omega^7 = 1$, $\omega^3 + \omega + 1 = 0$. БУ осуществляют умножение соответственно на ω и ω^3 в поле $GF(2^3)$. В рассматриваемом случае с выхода c_1 БУВ поступают нули, с выхода c_2 – последовательность управляющих сигналов $1\ \omega^3\ 1\ \omega^5\ 1\ \omega^3\ 1\ \omega^5\ \ldots$. Диаграмма переключений устройства состоит из двух циклов длиной 56 и длиной 8, как показано на рис. 6, *b*. На рис. 7 показаны схемы блоков умножения на ω и ω^3 в поле $GF(2^3)$.

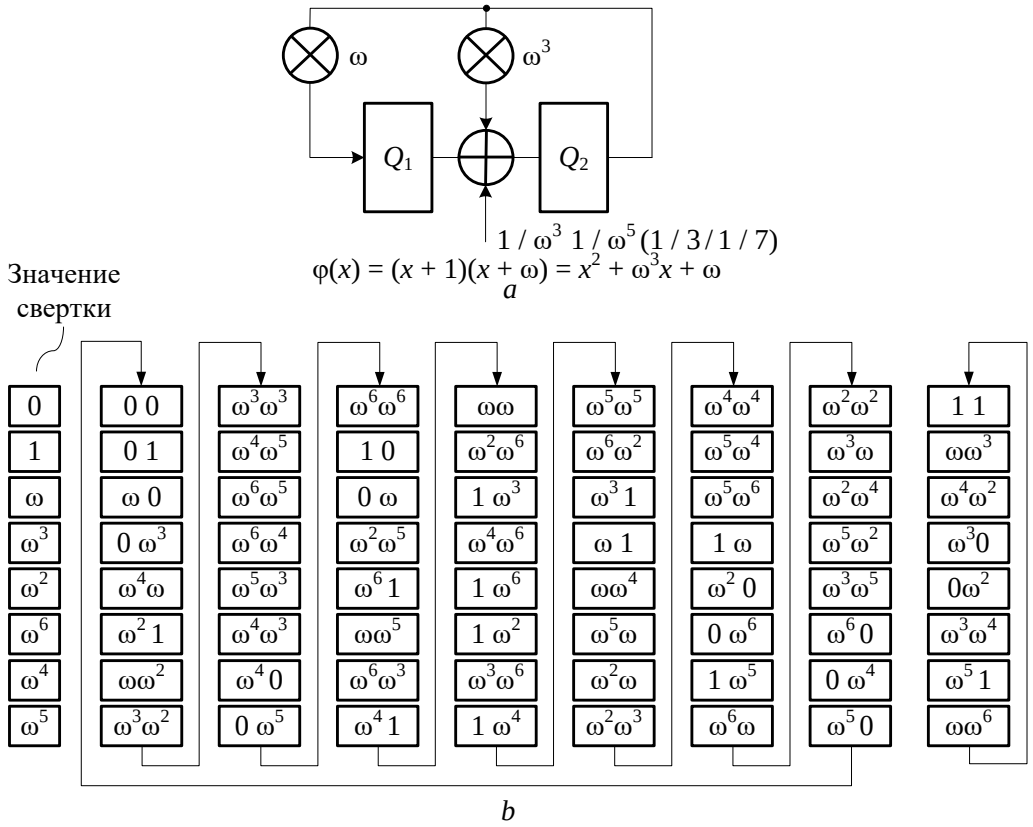
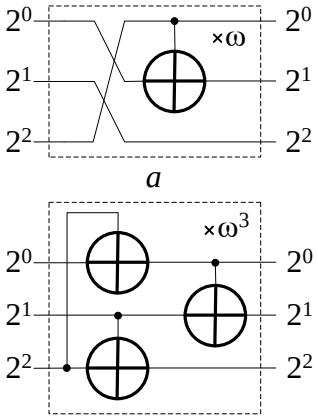


Рисунок 6 – Генератор (M – 7)-последовательностей при $n = 3$, $N = 2$: *a* – схема устройства; *b* – диаграмма 56-8 его переключений.



Входы	Выходы
000	000
001	010
010	100
011	110
100	011
101	001
110	111
111	101

c

Входы	Выходы
000	000
001	011
010	110
011	101
100	111
101	100
110	001
111	010

d

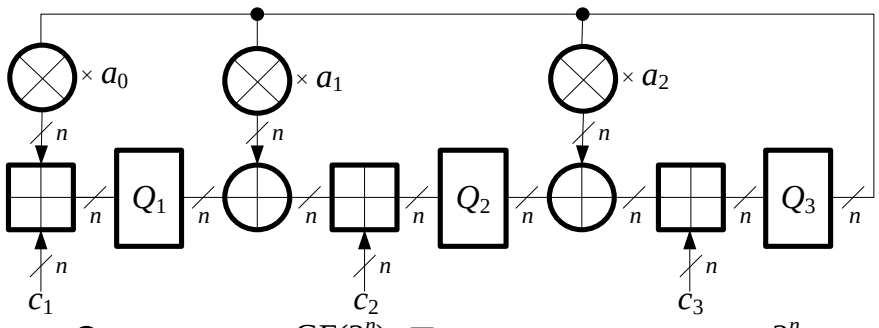
Рисунок 7 – Блоки умножения на ω и ω^3 в поле GF(2^3):
a, *b* – схемы блоков; *c*, *d* – соответствующие таблицы истинности.

За счет применения совершенно иного приема удалось синтезировать схему генератора (M – 1)-последовательностей, функционирующего в GF(2^n). Диаграмма переключений ГПСЧ в этом случае при правильно подобранных фиксированных значениях на управляющих входах состоит из двух циклов длиной $2^{nN} - 2$ и 2, где N – число регистров ГПСЧ, равное степени характеристического полинома особого вида $\varphi(x) = (x - 1)\lambda(x)$, где $\lambda(x)$ – полином, примитивный над GF(2^n). В рассматриваемом случае в схему вводятся сумматоры по модулю 2^n по числу ненулевых управляющих воздействий.

Выберем полином вида $\varphi(x) = (x + 1)\,\lambda(x)$, где $\lambda(x)$ – полином, примитивный над GF(2^n), и построим на его основе PRNG, уравнения работы которого имеют вид

$$\begin{cases} Q_1(t+1) = a_0 Q_N(t) \boxplus c_1, \\ Q_k(t+1) = a_{k-1} Q_N(t) \oplus Q_{k-1}(t) \boxplus c_k, \; k = 2, 3, 4, \ldots, N; \end{cases}$$

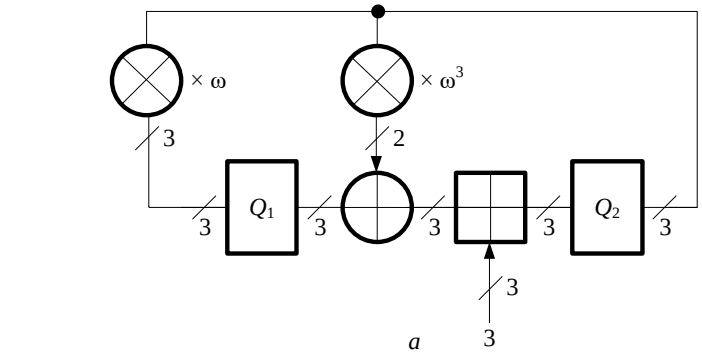
где $a_i \in$ GF(2^n) – коэффициенты полинома $\varphi(x)$ степени N, $c_i \in$ GF(2^n) – управляющие сигналы, $i = 1, 2, 3, \ldots, N$. На рис. 8 показан пример подобного генератора при $N = 3$.



⊕ - сложение в GF(2^n), ⊞ - сложение по модулю 2^n

Рисунок 8 – Схема генератора (M – 1)-последовательностей при $N = 3$.

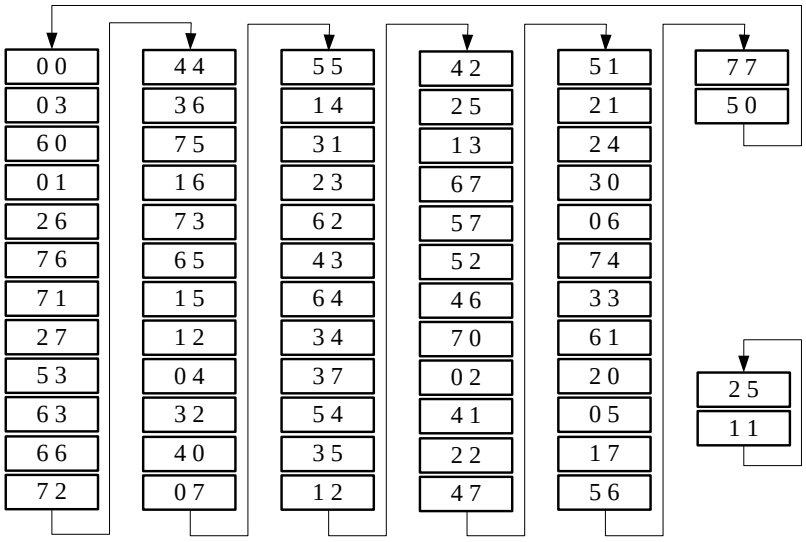
При правильном выборе значений управляющих сигналов c_i устройство формирует (M – 1)-последовательность. На рис. 9 показан пример генератора с диаграммой переключений 62-2.



a

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	$x^2 + 1$

b



c

Рисунок 9 – Схема генератора (M – 1)-последовательностей при n = 3, N = 2, $\varphi(x) = (x + 1)(x + \omega) = x^2 + \omega^3 x + \omega$: *a* – схема устройства; *b* – диаграмма переключений генератора при $c_1 = 0$, $c_2 = 3$.

Предложены и описаны методы перехода от генераторов последовательностей не максимальной длины всех рассмотренных типов к генераторам (M + 1)-последовательностей, т.е. последовательностей максимально возможной длины при заданном числе элементов памяти генератора.

Общая схема генератора (M + 1)-последовательностей, функционирующего в GF(2^n), показана на рис. 10. Селектор Sel анализирует состояние генератора и в тех случаях, когда надо изменить традиционный

порядок переключения элементов памяти, вырабатывает на своем выходе сигнал $z = 1$, который поступает на входы блоков коррекции Cor_i и инвертирует значение сигнала на входах соответствующих разрядов регистров q_i. Число блоков коррекции поддается минимизации. Так, например, при построении генератора $(M + 1)$-последовательностей на базе генераторов M- или $(M - 1)$-последовательностей можно обойтись только одним блоком коррекции.

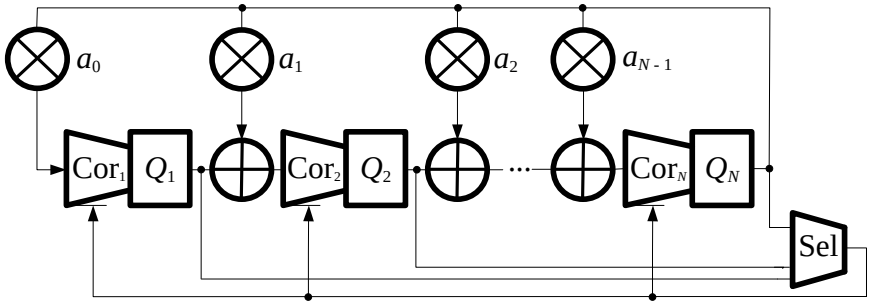


Рисунок 10 – Общая схема генератора $(M + 1)$-последовательностей, функционирующего в $\mathrm{GF}(2^n)$.

Если стоит задача синтеза на основе генератора M-последовательности, функционирующего в $\mathrm{GF}(2^n)$, генератора $(M + 1)$-последовательности, где $M = 2^{nN} - 1$, то алгоритм его построения имеет следующий вид.

Алгоритм 1 построения генератора $(M + 1)$-последовательности, где $M = 2^{n\,N} - 1$:

- Выбор характеристического полинома $\varphi(x)$ степени N, примитивного над $\mathrm{GF}(2^n)$;
- Синтез генератора, соответствующего выбранному $\varphi(x)$, и построение его диаграммы переключений, которая имеет вид $(2^{nN} - 1)$-1;
- Выбор состояния Ω_1 генератора, принадлежащего кодовому кольцу длиной $2^{nN} - 1$ диаграммы переключения, из которого будет осуществляться переход в ранее запрещенное состояние Ω_0;
- Синтез селектора, на выходе которого формируется сигнал $z = 1$, когда генератор оказывается в состоянии Ω_1 или в состоянии Ω_0; иначе говоря,

$$z = ((q_1 q_2 \ldots q_N) = \Omega_1) \text{ OR } ((q_1 q_2 \ldots q_N) = \Omega_0);$$

- Ввод в схему генератора блока коррекции (БК) на элементах XOR, которые инвертируют сигналы на входах соответствующих элементов памяти генератора, обеспечивая его переход из состояния Ω_1 в состояния Ω_0, а затем переход из состояния Ω_0 в состояние Ω_2, следующее за состоянием Ω_1 в устройстве-прототипе.

При этом в тех случаях, когда состояния Ω_1 и Ω_0 отличаются друг от друга только в одном разряде одного из регистров схемы блока коррекции и селектора будут максимально простыми (соответственно один двухвходовой элемент XOR и один (nN – 1)-входовой вентиль AND или NOR).

На рис. 11 показан пример построения генератора (M + 1)-последовательности на основе генератора M-последовательности для ситуации, когда n = 2, N = 2, $\varphi(x) = x^2 + x + \omega$. В рассматриваемом случае Ω_0 = 00, Ω_1= 10, Ω_2 = 01.

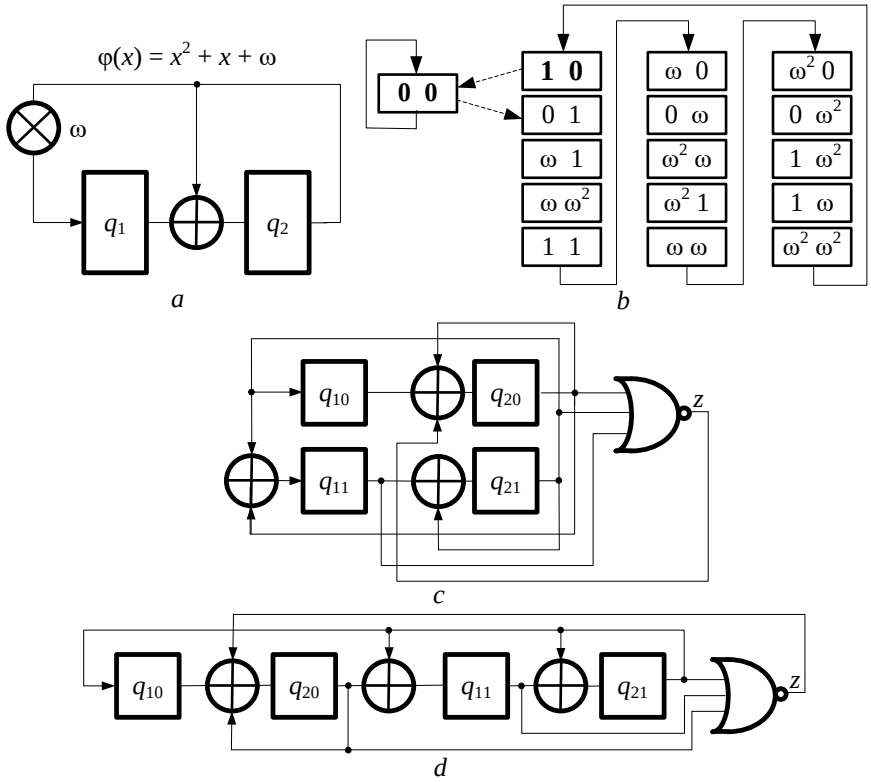


Рисунок 11 – Схема генератора (M + 1)-последовательностей:
a – схема устройства-прототипа, соответствующего $\varphi(x) = x^2 + x + \omega$ при n = 2, N = 2; *b* – идея построения генератора (M + 1)-последовательностей; *c*, *d* – две эквивалентные схемы генератора последовательности длиной 16.

Если стоит задача синтеза на основе генератора (M – 1)-или ($M - 2^n$ + 1)-последовательности, функционирующего в GF(2^n), генератора (M + 1)-последовательности, алгоритм его построения имеет следующий вид.

Алгоритм 2 построения генератора (M + 1)-последовательности, где $M = 2^{nN} - 1$:

– Выбор характеристического полинома степени N вида $\varphi(x) = (x + 1)\lambda(x)$, где $\lambda(x)$ – полином, примитивный над GF(2^n);
– Синтез генератора, соответствующего выбранному $\varphi(x)$, и построение его диаграммы переключений;

– Выбор состояния Q_1 генератора, принадлежащего большему кодовому кольцу диаграммы переключения, из которого будет осуществляться переход в состояние Q_4 меньшего кодового кольца;
– Выбор состояния Q_3 генератора, принадлежащего меньшему кодовому кольцу диаграммы переключения и предшествующего состоянию Q_4, из которого будет осуществляться возврат в состояние Q_2 большего кодового кольца, следующего за состоянием Q_1 в устройстве-прототипе;
– Синтез селектора, на выходе которого формируется сигнал $z = 1$, когда генератор оказывается в состоянии Q_1 или в состоянии Q_3; иначе говоря,

$$z = ((q_1 q_2 \ \ldots \ q_N) = Q_1) \text{ OR } ((q_1 q_2 \ \ldots \ q_N) = Q_3);$$

– Ввод в схему генератора блоков коррекции (БК) на элементах XOR, которые инвертируют сигналы на входах соответствующих элементов памяти генератора, обеспечивая его переход из состояния Q_1 в малое кодовое кольцо и возврат из состояния Q_3 в большое кодовое кольцо диаграммы переключений.

При этом в тех случаях, когда состояния Q_2 и Q_4 отличаются друг от друга только в одном разряде одного из регистров схема блока коррекции, будет максимально простой и состоять только из одного двухвходового элемент XOR.

На рис. 12 показан пример построения генератора $(M + 1)$-последовательности на основе генератора $(M – 1)$-последовательности для случая $n = 2$, $N = 2$, $\varphi(x) = (x + 1)(x + \omega) = x^2 + \omega^2 x + \omega$. В рассматриваемом случае $Q_1 = 13$, $Q_2 = 10$, $Q_3 = 23$, $Q_4 = 11$.

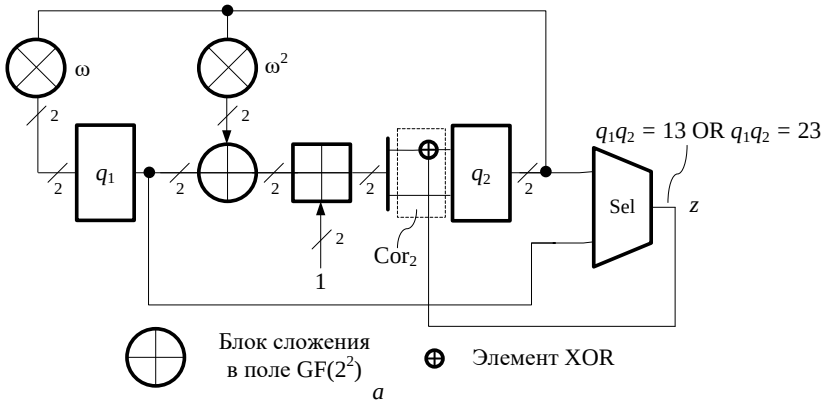


Рисунок 12 – Схема генератора (M + 1)-последовательностей: a – схема устройства-прототипа, соответствующего $\varphi(x) = x^2 + \omega^2 x + \omega$ при $n = 2$, $N = 2$; b – идея построения генератора (M + 1)-последовательностей; c – вариант схемы селектора.

В *третьей главе* дается информация о разработанных программных моделях новых типов ГПСЧ, рассмотренных в главе 2, приводятся результаты исследования их свойств.

Рассмотрим результаты исследований генераторов ($M - 2^n + 1$)-последовательностей. Исходная информация для моделирования: порядок n поля GF(2^n), степень N характеристического полинома, коэффициенты обратной связи $a_0\ a_1\ a_2\ \ldots\ a_{N-1}$, управляющие воздействия $c_1\ c_2\ c_3\ \ldots\ c_N$. Выходная информация: длины циклов диаграммы переключений, включающей в себя все 2^{nN} состояний генератора, а также состояния генератора, входящие в эти циклы.

В качестве примера рассмотрим результаты моделирования генераторов, функционирующих в поле GF(2^3).

Выявлено, что

1) генераторы ($M - 2^3 + 1$)-последовательностей существуют только при длине управляющих воздействий $L \in \{4, 8\}$;
2) каждое найденное УВ длиной L позволяет определить целое семейство из 2^3 генераторов ($M - 2^3 + 1$)-последовательностей, имеющих различные диаграммы переключений и формируемых при фиксированном УВ но при различных векторах инициализации $IV = \Sigma_{\text{нач}}$;
3) при $L = 4$ генераторы ($M - 2^3 + 1$)-последовательностей существуют тогда и только тогда, когда УВ имеют вид либо 1 / α / 1 / β, либо α / 1 / β / 1, где $\alpha \in$ GF(2^3), $\beta \in$ GF(2^3), $\alpha \neq \beta$.

Очевидно, что свойство 2 справедливо при любом порядке n поля GF(2^n).

На рис. 13 показано семейство генераторов ($M - 2^3 + 1$)-последовательностей, порождаемое УВ длиной 4 вида $1 / \omega^3 / 1 / \omega^5$. На рис. 14 показана последовательность вычисления значений свертки в GF(2^n) при заданных значениях вектора инициализации (IV) и управляющего воздействия. На рис. 15 показан законы изменения значений свертки в GF(2^3) для некоторых управляющих воздействий длиной 8, обеспечивающих формирование ($M - 7$)-последовательностей. На рис. 16 показан закон изменения значений свертки в GF(2^3) при различных значениях векторов инициализации ГПСЧ для некоторых управляющих воздействиях длиной 4 вида 1 / α / 1 / β или α / 1 / β / 1, обеспечивающих формирование ($M - 7$)-последовательностей.

На рис. 17 показана схема алгоритма выявления УВ, порождающих генераторы ($M - 2^n + 1$)-последовательностей при произвольном порядке n поля GF(2^n).

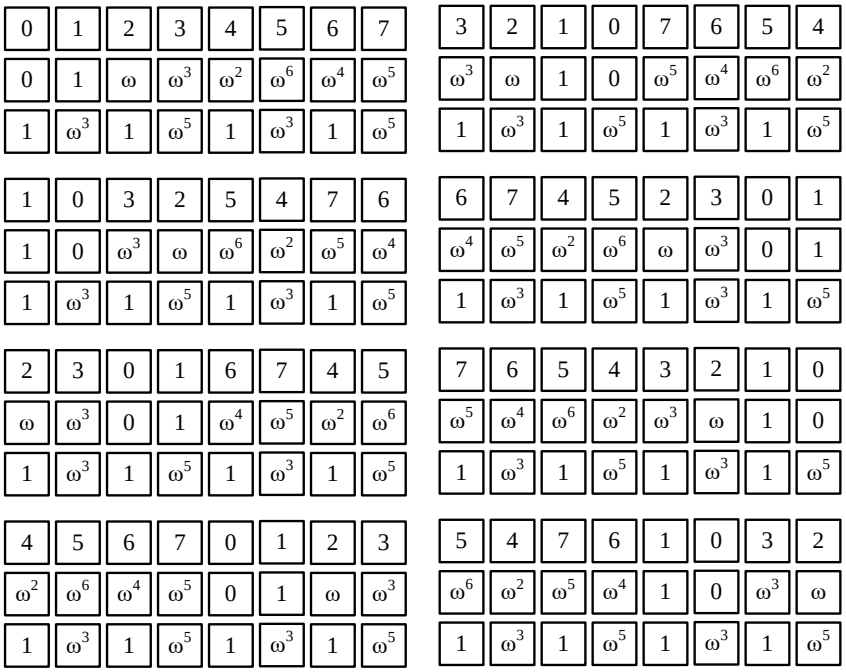


Рисунок 13 – Закон изменения значений свертки в GF(2^3) при различных значениях векторов инициализации (ВИ) ГПСЧ для управляющего воздействия длиной 4 вида 1 / ω^3 / 1 / ω^5, обеспечивающего формирование (M – 7)-последовательностей. Первые две строки – это закон изменения свертки, третья – управляющие воздействия.

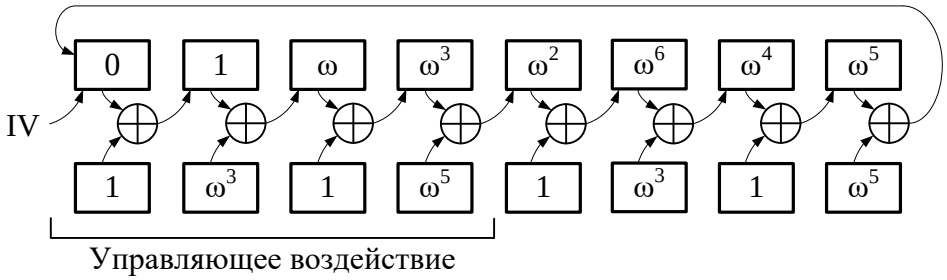


Рисунок 14 – Последовательность вычисления значений свертки в GF(2^n) при заданных значениях ВИ (IV) и последовательности управляющих воздействий.

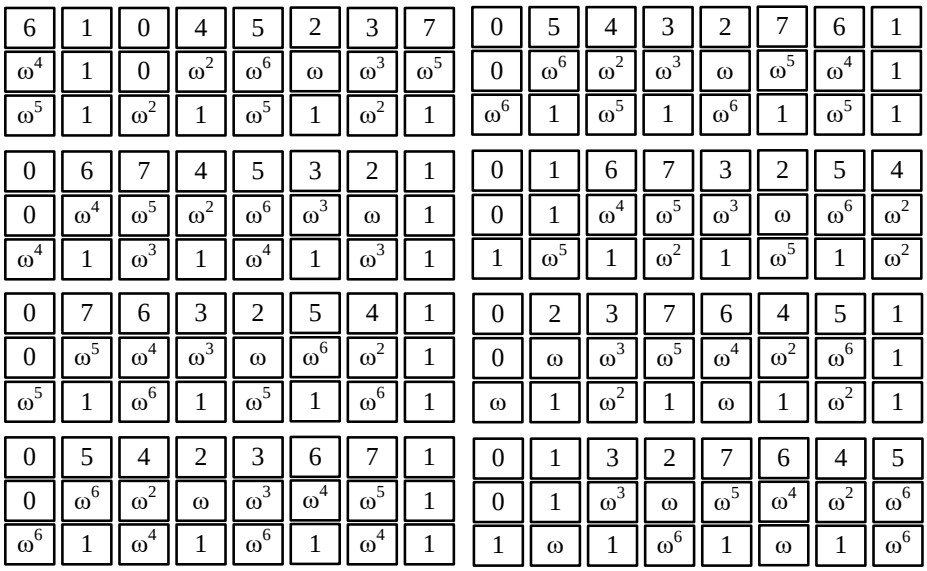


Рисунок 15 – Закон изменения значений свертки в GF(2^3) при различных значениях ВИ для последовательностей УВ длиной 4 вида 1 / α / 1 / β и α / 1 / β / 1, обеспечивающих формирование (*M* – 7)-последовательностей.

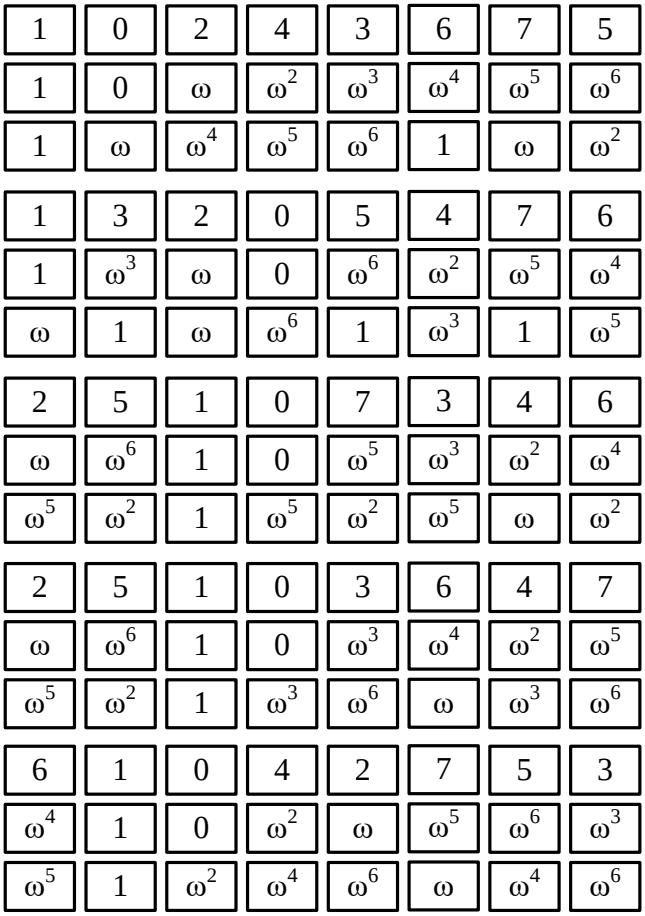


Рисунок 16 – Закон изменения значений свертки в GF(2^3) при различных значениях ВИ и УВ длиной 8, обеспечивающих формирование (*M* – 7)-последовательностей.

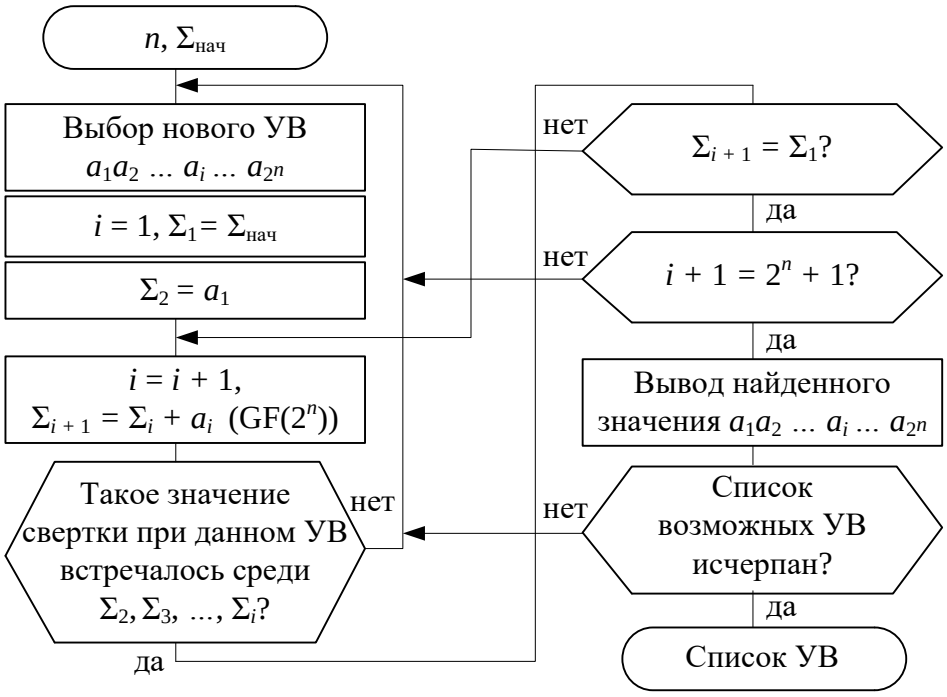


Рисунок 17 – Схема алгоритма поиска управляющих воздействий (УВ), обеспечивающих формирование ($M – 2^n + 1$)-последовательностей.

Рассматриваются вопросы программной и аппаратной реализации вычислений в конечных полях GF(2^n). Рассматриваются операции умножения и нахождения мультипликативной инверсии элементов поля.

Предлагается следующий алгоритм нахождения примитивных элементов поля GF(q), где $q = p^n$:

- Определение количества примитивных элементов GF(q) по формуле $N_\omega = \psi(q - 1)$, где $\psi(\cdot)$ – число Эйлера;
- Составление списка чисел m_i, меньших $q - 1$ и удовлетворяющих условию $gcd(m_i, q - 1) = 1$, $i = 1, 2, \ldots, N_\omega$;
- Нахождение первого примитивного элемента ω_1;
  - для полей GF(p^n), порождаемых примитивным полиномом $\varphi(x)$, $\omega_1 = x$;
  - для полей GF(2^n), порождаемых не примитивным полиномом $\varphi(x)$, $\omega_1 = x + 1$;
  - для всех остальных полей ω_1 находится полным перебором;
- Определение оставшихся примитивных элементов по формуле

$$\omega_j = \omega_1^{m_j} \bmod \varphi(x), j = 2, 3, ..., N_\omega.$$

На рис. 18 иллюстрируется принцип построения БУ по виду сопровождающей матрицы T_i на примере поля GF(2^3).

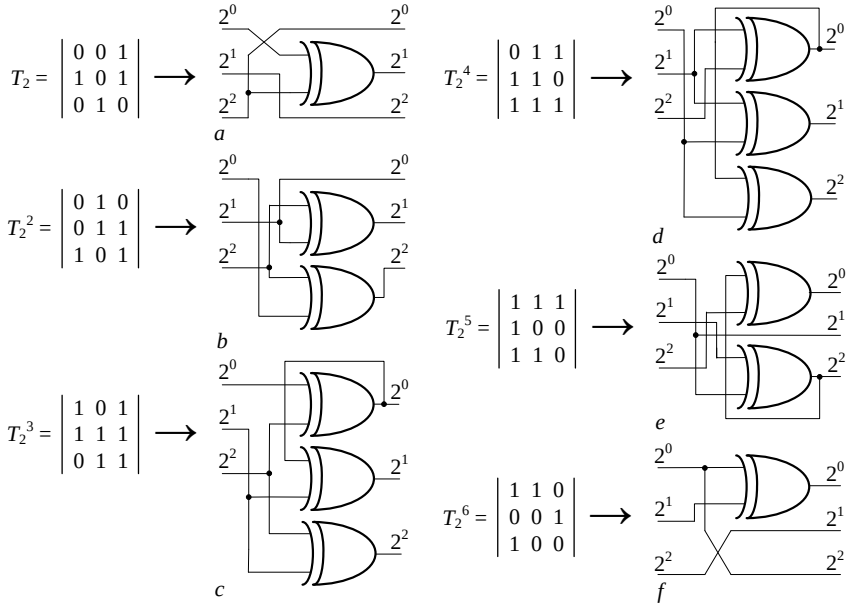


Рисунок 18 – Схемы блоков умножения в GF(2^3): *a* – блок умножения на ω; *b* – блок умножения на ω^2; *c* – блок умножения на ω^3; *d* – блок умножения на ω^4; *e* – блок умножения на ω^5; *f* – блок умножения на ω^6.

В *четвертой главе* рассматриваются вопросы повышения эффективности стохастических алгоритмов обработки данных.

Цифровые устройства (ЦУ) все чаще используются в тех приложениях, где требуется высокая надежность функционирования. Известные методы аппаратного контроля ЦУ в реальном масштабе времени, такие как дублирование, контроль с использованием корректирующих кодов и другие, требуют значительных аппаратных затрат на их реализацию.

Представлен метод построения самопроверяемого ГПСЧ. Метод основан на использовании характеристического полинома специального вида и предсказании значения свертки содержимого элементов памяти генератора. Одна из возможных областей применения метода – синтез синхронных самопроверяемых счетчиков.

В двоичных генераторах Галуа, соответствующих $\varphi(x) = (x + 1)\lambda(x)$, где $\lambda(x)$ – полином, примитивный над GF(2), и генераторах с диаграммой переключений (2^{N-1})-(2^{N-1}), построенных на их основе, свертка по модулю два содержимого всех разрядов при корректной работе устройства не меняет своего значения. Это свойство позволяет организовать самоконтроль, уравнение которого имеет вид

$$\sum_{i=1}^{N} q_i(t+1) \pmod 2 = \sum_{i=1}^{N} q_i(t) \pmod 2.$$

В двоичных генераторах $(M - 1)$-последовательностей, свертка по модулю два содержимого всех разрядов при корректной работе устройства в каждом такте меняет свое значение. Это свойство позволяет организовать самоконтроль, уравнение которого имеет вид

$$\sum_{i=1}^{N} q_i(t+1) \pmod 2 = \sum_{i=1}^{N} q_i(t) + 1 \pmod 2.$$

Рассмотрим вопрос организации самоконтроля для недвоичных ГПСЧ. Для генераторов, функционирующего в GF(p), где p – простое, как было показано в главе 2, можно построить генератор (M – p + 1)-последовательности, в каждом такте которого значение свертки содержимого регистров которого меняется на a, где $a \in \mathrm{GF}(p)$, $a \neq 0$. Таким образом, уравнение самоконтроля для генератора (M – p + 1)-последовательности будет иметь вид

$$\sum_{i=1}^{N} q_i(t+1) \pmod p = \sum_{i=1}^{N} q_i(t) + a \pmod p.$$

Схема самоконтроля показана на рис. 19.

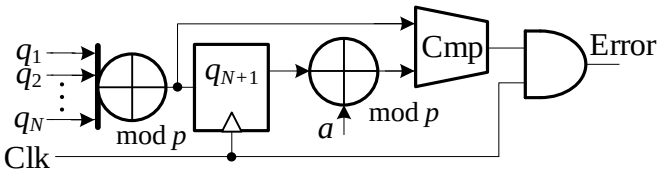


Рисунок 19 – Организация самоконтроля p-ичных PRNG, p – простое, когда свертка по модулю p содержимого всех регистров генератора при корректной работе в каждом такте меняет свое значение на a.

В общем случае диаграмма переключений генератора (M – p + 1)-последовательностей имеет вид (p^N – p)-p. При построении генератора (M + 1)-последовательностей на основе генератора (M – p + 1)-последовательностей, и сохранением закона изменения значения свертки содержимого регистров ГПСЧ, уравнение самоконтроля остается в силе.

В последние годы серьезной проблемой стало вредоносное аппаратное обеспечение (Malicious Hardware). Из-за аутсорсинга в процессе изготовления интегральных схем (ИС) появляются проблемы, связанные с внедрением аппаратных закладок, подделками ИС, пиратством и несанкционированным перепроизводством. Наиболее эффективные возможности по предотвращению всех вышеперечисленных угроз предоставляют технологии Logic Encryption и Design Obfuscation.

Рассмотрим кратко суть первой из них. Обфускация логической схемы ЦУ (рис. 20) дает возможность использовать дополнительные логические элементы в структуре ИС, чтобы скрыть ее оригинальные функциональные возможности. Иначе говоря, это попытка максимально усложнить понимание логики работы защищаемой схемы для неавторизованных лиц. Обфускация логической схемы (меняет конструкцию ИС таким образом, что она работает правильно, только в том случае, если сигналы на дополнительных ключевых входах устройства принимают правильные значения. На рис. 20, *b* показана модифицированная схема обфускации, предполагающая использование дополнительной схемы

преобразования ключей, реализованной на основе блока памяти с защитой от НСД. Этот блок памяти устанавливается или активируется на заключительном этапе создания ИС перед ее продажей конечному потребителю.

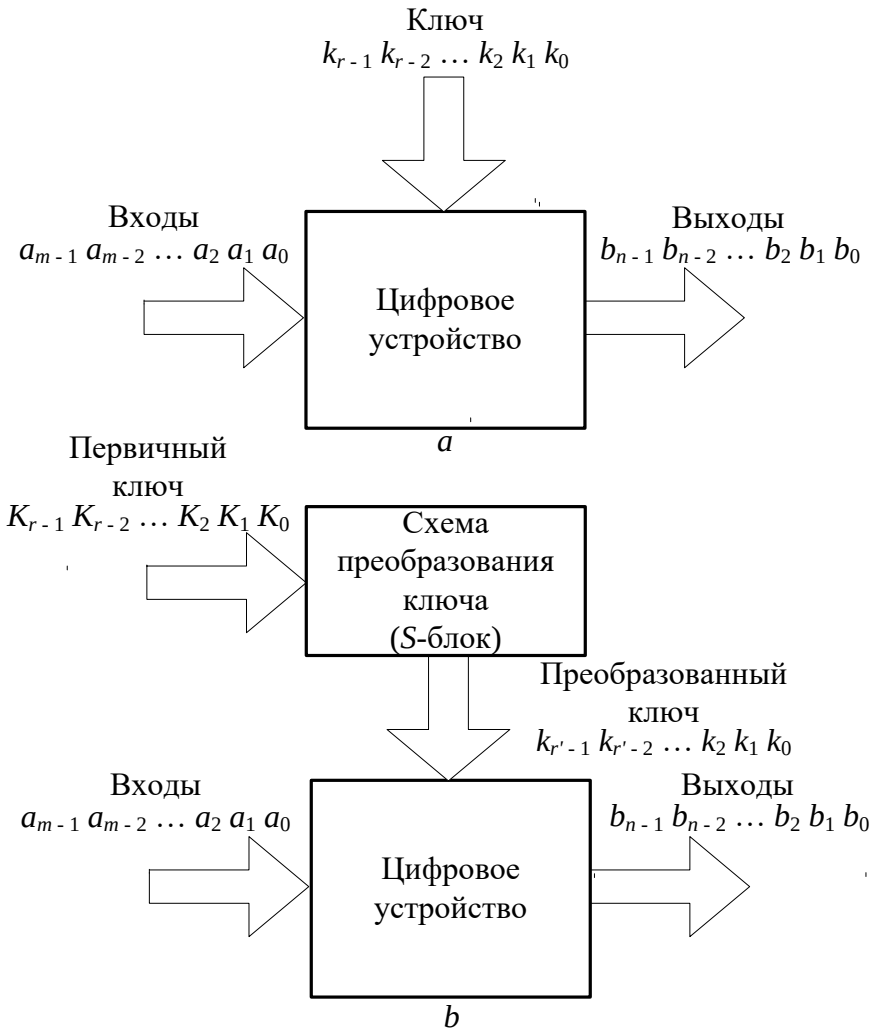


Рисунок 20 – Обфускация логической схемы ЦУ:
a – вариант 1 без использования схемы преобразования ключа;
b – вариант 2 с использованием схемы преобразования ключа.

На практике применение идеи запутывания логической схемы устройства помимо решения вышеперечисленных проблем позволяет реализовать механизм скрытых (особо защищенных) функций устройства, например, для защиты технического решения от использования по двойному назначению.

На рис. 21 показана разработанная схема четырехразрядного генератора с десятью ключевыми входами, а значит способная выполнять 2^{10} различных функций. На рис. 22 приведена эквивалентная схема генератора в одном из режимов и соответствующая диаграмма переключений.

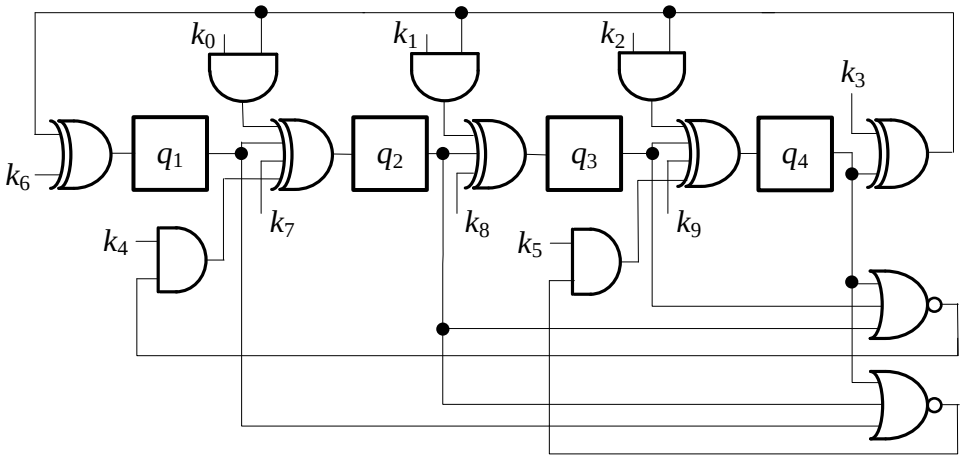


Рисунок 21 – Схема двоичного четырехразрядного PRNG.

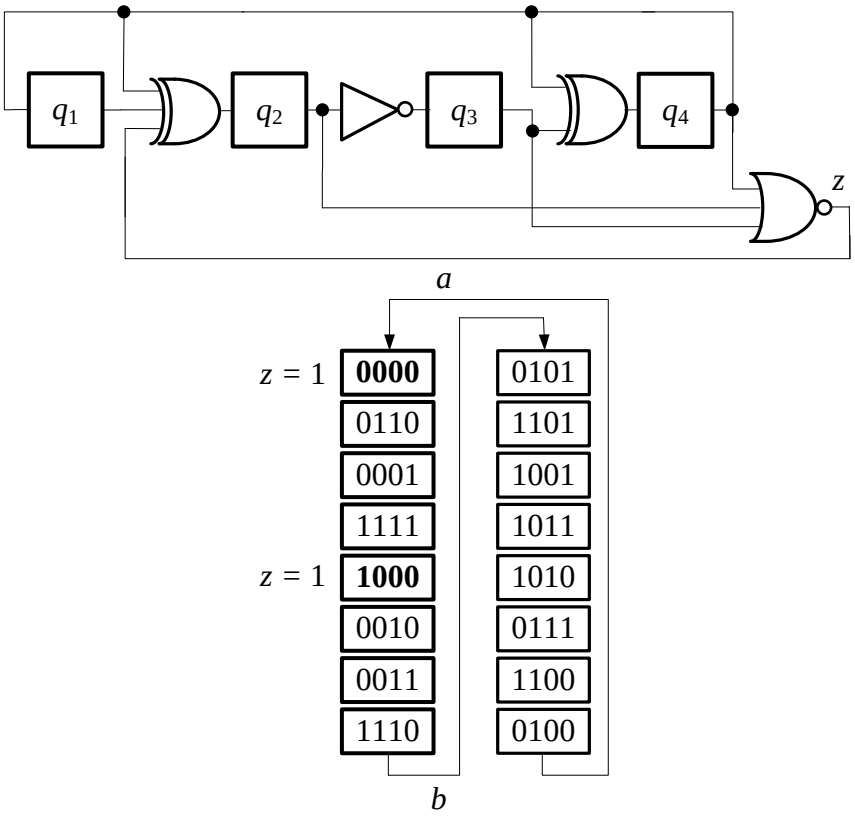


Рисунок 22 – Логика работы двоичного четырехразрядного генератора при $k_9\ k_8\ k_7\ k_6\ k_5\ k_4\ k_3\ k_2\ k_1\ k_0$ = 0 1 0 0 0 1 0 1 0 1:
a – эквивалентная схема устройства; *b* – диаграмма его переключений.

В *заключении* отражены основные результаты, полученные в диссертационной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Целью работы являлось повышение эффективности стохастических алгоритмов за счет увеличения периода формируемых последовательностей, исключения линейных зависимостей между отдельными фрагментами недвоичных псевдослучайных последовательностей (ПСП), обеспечения возможности самоконтроля правильности функционирования генераторов псевдослучайных чисел (ГПСЧ), разработки схем генераторов, ориентированных на реализацию технологий Design Obfuscation и Logic Obfuscation.

Основные результаты:

1) Разработан метод построения ГПСЧ, обеспечивающих формирование последовательностей максимально возможной длины при заданном количестве элементов памяти, так называемых генераторов $(M + 1)$-последовательностей для всех новых типов генераторов последовательностей не максимальной длины.
2) Показано, что методы, позволяющие синтезировать генераторы $(M – p + 1)$-последовательностей на базе ГПСЧ, функционирующих в поле $GF(p)$, где p – простое, имеющих диаграмму переключений вида $(p^N – p)$-p, где N – степень характеристического полинома особого вида, для случая расширенных полей вида $GF(p^n)$, где n – натуральное, не работают. Разработаны математическая и программная модели и схема генератора $(M – 2^n + 1)$ -последовательностей на базе ГПСЧ, функционирующих в поле $GF(2^n)$. Особенностью разработанных генераторов является использовании блока управляющих воздействий (БУВ), при этом не на всех своих выходах БУВ формирует фиксированные значения управляющих сигналов, как это имеет место в случае поля $GF(p)$. Также стоит отметить, что состояния генератора, попадающие в малое кодовое кольцо диаграммы переключений, зависят от вида управляющих воздействий с выхода БУВ и от начального состояния ГПСЧ. Это расширяет функциональные возможности генератора при его использовании для реализации технологии Design Obfuscation.
3) Разработаны математическая и программная модели и схема генератора $(M – 1)$-последовательностей на базе ГПСЧ, функционирующих в поле $GF(2^n)$. Особенностью разработанных генераторов является использовании блоков сложения по модулю 2^n, при этом на всех управляющих входах присутствуют фиксированные значения управляющих сигналов. Диаграмма переключений генератора имеет вид $(2^{nN} – 2)$-2. Как и в предыдущем случае можно отметить, что состояния генератора, попадающие в малое кодовое кольцо диаграммы переключений, зависят от вида

управляющих воздействий и от начального состояния ГПСЧ. Появление в схеме генератора блоков сложения по модулю 2^n повышает степень нелинейности закона формирования выходной последовательности. Это позволяет использовать генератор для реализации ARX-алгоритмов стохастического преобразования данных.

4) Продемонстрирована эффективная аппаратная и программная реализация вычислений в GF(2^n). Представлены схемы алгоритмов и примеры нахождения произведения элементов GF(2^n), как табличным способом, так и вычислением «на лету»; мультипликативной инверсии в GF(2^n); определения примитивных элементов GF(p^n). Представлен алгоритм построения блоков умножения в GF(2^n) на основе использования сопровождающей матрицы. Разработанный алгоритм определения примитивных элементов GF(p^n) ориентирован на решение задачи построения генератора ненулевых элементов GF(2^n), необходимого для определения соответствия различных форм представления элементов поля.
5) Разработанные программные модели генераторов ($M - p + 1$)-, ($M - 2^n + 1$)- и ($M - 1$)-последовательностей позволили провести исследование их технических характеристик. Определены управляющие воздействия (УВ), которые позволяют получить ПСП требуемого вида. Каждое выявленное УВ длиной позволяет определить целое семейство из 2^n генераторов ($M - 2^n + 1$)-последовательностей, имеющих различные диаграммы переключений и формируемых при фиксированном УВ, но при различных векторах инициализации. Определены законы изменения свертки содержимого регистров генераторов в процессе их функционирования. Выявлено, что структура выходных последовательностей генераторов ($M - 2^n + 1$)- и ($M - 1$)-последовательностей такова, что отсутствуют линейные зависимости между фрагментами ПСП, что позволяет использовать эти последовательности на всей длине периода в отличии от параллельных двоичных и последовательных и параллельных генераторов M-последовательностей.
6) По результатам моделирования генераторов ($M - 2^n + 1$)-последовательностей сформулирована гипотеза о том, что эти генераторы существуют только при длине УВ $L \in \{2^{n-1}, 2^n\}$.
7) Предложен метод построения самопроверяемых ГПСЧ. Метод основан на использовании характеристических полиномов специального вида и предсказании значения свертки содержимого элементов памяти генератора. Одна из возможных областей применения метода – синтез синхронных самопроверяемых счетчиков. К сожалению, саму схему самоконтроля в текущей реализации нельзя признать самопроверяемой, так как она является одновы-

ходной. В результате константная неисправность выхода контролирующей схемы не обнаруживается. В идеальном случае схема самоконтроля должна иметь как минимум два выхода.

8) Предложена конструкция 3D хеш-генератора, особенностью которого является высокая степень параллелизма на уровне элементарных преобразований. Хеш-генератор ориентирован на использования в качестве примитива при реализации стохастических алгоритмов обработки данных более высокого уровня.
9) В рамках исследования технологии Logic Encryption проработан вопрос запутывания логической схемы ГПСЧ для защиты от реверс-инжиниринга. Предложена схема четырехразрядного генератора с десятью ключевыми входами, а значит способная выполнять 2^{10} различных функций. Предложен способ реализации механизма скрытых функций на основе использования генераторов (M – 2^n + 1)- и (M - 1)-последовательностей

Главное достоинство разработанного семейства ГПСЧ – структура выходной последовательности принципиально отличается от классической. Их выходные последовательности можно использовать на всей длине периода.

В качестве направлений дальнейших исследований можно выделить разработку метода запутывания логической схемы ГПСЧ на основе возможности изменения базового конечного поля; разработку полностью самопроверяемой схемы самоконтроля ГПСЧ, имеющей более одного выхода; исследование зависимости числа реализуемых функций ГПСЧ от числа элементов памяти генератора; разработку схемы ГПСЧ, ориентированного на реализацию технологии Design Obfuscation; разработку схемы ГПСЧ с защитой от использования по двойному назначению и наконец исследование предложенных генераторов (M + 1)-последовательностей по методике НИСТ.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ ОТРАЖЕНО В СЛЕДУЮЩИХ ОПУБЛИКОВАННЫХ РАБОТАХ

1. Иванов М.А., Коннова И.Г., Саликов Е.А., Степанова М.А. Обфускация логических схем генераторов псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. // Безопасность информационных технологий, 2021 г., Том 28, № 1, с. 74-83.
2. Иванов М.А., Комаров Т.И., Саликов Е.А., Чепик Н.А. Хеш-функция на основе 3D стохастических преобразований // Информационные войны, 2019, № 4(52), с. 71-76.
3. Иванов М.А., Саликов Е.А. Генератор псевдослучайных чисел. Патент РФ на изобретение № 2 740 339, Бюл. № 2, 13.01.2021.
4. Иванов М.А., Саликов Е.А. Способ хеширования информации. Патент РФ на изобретение № 2 747 517, Бюл. № 13, 06.05.2021.

5. Иванов М.А., Саликов Е.А., Степанова М.А. Генератор псевдослучайных чисел. Патент РФ на изобретение № 2 756 833, Бюл. № 28, 06.10.2021.
6. Иванов М.А., Саликов Е.А., Козлов А.А., Григорьев М.П., Хисамутдинов М.А., Чуркин К.Ю. Генератор псевдослучайных чисел. Патент РФ на изобретение № 2776346, Бюл. № 20, 19.07.2022.
7. M. Ivanov, I. Chugunkov, B. Kliuchnikova, and E. Salikov. (M + 1)-Sequence Generators with Concurrent Error Detection // Procedia Computer Science, 2021, Vol. 190, Q2, pp. 361-369.
8. M. Ivanov, I. Chugunkov, B. Kliuchnikova, and E. Salikov. Encryption of pseudorandom number generator logic circuits // Procedia Computer Science, 2021, Vol. 190, Q2, pp. 370-376.
9. M. Ivanov, T. Komarov, E. Salikov and N. Chepik. GDozenHash Hash Function Based on Three-Dimensional Stochastic Transformations. // Mechanisms and Machine Science, 2020, Vol. 80, Q3, pp. 375-385.
10. I.V. Chugunkov, B.V. Kliuchnikova, M.A. Ivanov, E.A. Salikov and A.O. Zubtsov. New Class of Pseudorandom Number Generators for Logic Encryption Realization. // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020, pp. 271-273.
11. M.A. Ivanov, B.V. Kliuchnikova, E.A. Salikov and A.V. Starikovskii. New Class of Non-binary Pseudorandom Number Generators. // Mechanisms and Machine Science, 2020, Vol. 80, pp. 291-298.
12. A.V. Zelenoritskaya, M.A. Ivanov and E.A. Salikov. Possible Modifications of RC4 Stream Cipher. // Proceedings of Intelligent Technologies in Robotics, Moscow, Russia, 2020, Vol. 80, pp. 335-341.
13. I.V. Chugunkov, L.D. Gatilova, M.A. Ivanov, B.V. Kliuchnikova, A.A. Kozlov, and E.A. Salikov. Computing in Finite Fields. // Proceedings of the 2022 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2022, pp. 273-276.
14. Иванов М.А., Саликов Е.А. Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. Учебное пособие. – М.: НИЯУ МИФИ, 2021.
15. Генераторы псевдослучайных чисел в задачах защиты информации. Учебное пособие. Иванов М.А., Саликов Е.А., Стариковский А.В., Чукова Д.И. – М.: РГУ нефти и газа им. И.М. Губкина., 2021.