

4859348

На правах рукописи

Сухинин Борис Михайлович

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ВЫСОКОСКОРОСТНЫХ
ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ РАВНОМЕРНО
РАСПРЕДЕЛЕННЫХ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА
ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

05.13.17 — Теоретические основы информатики

10 НОЯ 2011

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Сух -

Москва – 2011

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования
«Московский государственный технический университет имени
Н. Э. Баумана» (МГТУ им. Н. Э. Баумана)

Научный руководитель:	канд. физ.-мат. наук Жуков Алексей Евгеньевич
Официальные оппоненты:	д-р физ.-мат. наук, проф. Грушо Александр Александрович канд. техн. наук Архангельская Анна Васильевна
Ведущая организация:	Национальный исследовательский ядерный университет «МИФИ»


Защита диссертации состоится 8 декабря 2011 г. в 14 часов 30 минут на заседании диссертационного совета Д 212.141.10 при МГТУ им. Н. Э. Баумана по адресу: 105005, г. Москва, ул. 2-я Бауманская, д. 5, стр. 1.

Отзыв на автореферат, заверенный печатью организации, просим высылать по адресу: 105005, г. Москва, ул. 2-я Бауманская, д. 5, стр. 1, МГТУ им. Н. Э. Баумана, ученому секретарю совета Д 212.141.10.

С диссертацией можно ознакомиться в библиотеке МГТУ им. Н. Э. Баумана.

Автореферат разослан «___» _____ 2011 г.

Ученый секретарь диссертационного совета,
канд. техн. наук, доцент

 С. Р. Иванов

Диссертационная работа посвящена разработке новых методов генерации псевдослучайных равномерно распределенных двоичных последовательностей, основанных на использовании клеточных автоматов. К основным достоинствам разработанных методов относятся контролируемый период и хорошие статистические свойства псевдослучайных последовательностей, эффективность и высокое быстродействие аппаратной реализации генераторов.

Актуальность проблемы. Актуальность обусловлена широким применением псевдослучайных последовательностей в имитационном моделировании, методах Монте-Карло, криптографии, программировании и иных областях. Свой вклад в исследование псевдослучайных последовательностей и их генераторов внесли такие известные ученые, как А. Н. Колмогоров, Р. фон Мизес, Дж. фон Нейман, Дж. Марсалья, Д. Кнут, П. Лекваер, С. Вольфрам и др. Вопросы генерации псевдослучайных последовательностей широко обсуждаются на отечественных и зарубежных научных конференциях, таких как *MCQMC*, *The Winter Simulation Conference*, *Crypto*, *EuroCrypt*, *FSE*, *CHES*, *Sibecrypt*, *РусКрипто* и т. д.

По мере развития возможностей вычислительной техники разрыв между предъявляемыми требованиями и возможностями существующих генераторов неуклонно возрастает. Проведенный в рамках диссертационного исследования обзор показал, что основной проблемой при разработке генераторов псевдослучайных последовательностей является сочетание высокого быстродействия, эффективности реализации и хороших статистических свойств.

К перспективным направлениям исследований относится разработка новых методов генерации псевдослучайных последовательностей, рассчитанных на реализацию на параллельных вычислительных устройствах, что связано со сменой парадигмы вычислительного процесса и переходом от последовательных вычислений к параллельным. При этом задача генерации случайной последовательности с заданным законом распределения может быть сведена к задаче генерации случайной равномерно распределенной двоичной последовательности.

Цель и задачи. Целью исследований являлась разработка новых генераторов псевдослучайных равномерно распределенных двоичных последовательностей, отвечающих следующим требованиям:

- выходные последовательности генераторов на длине периода должны быть статистически неотличимы от случайных равномерно распределенных двоичных последовательностей, что должно подтверждаться успешным прохождением соответствующих специализированных тестов;
- период выходных последовательностей генераторов должен превосходить требуемые на практике значения;

- быстроедействие и эффективность реализации генераторов на параллельных вычислительных устройствах, таких как ПЛИС, должны быть не ниже, чем у известных аналогов.

При этом исследования были изначально ограничены рассмотрением генераторов, основанных на использовании клеточных автоматов.

Для достижения поставленной цели были решены следующие задачи:

- проведен обзор наиболее распространенных генераторов псевдослучайных последовательностей, выявлены их основные достоинства и недостатки, рассмотрены методы улучшения статистических свойств выходных последовательностей;
- исследованы свойства клеточных автоматов;
- осуществлен синтез структуры и обоснован выбор параметров генераторов псевдослучайных последовательностей на основе клеточных автоматов;
- экспериментально исследованы статистические свойства выходных последовательностей разработанных генераторов и подтверждено их соответствие предъявленным требованиям;
- разработана аппаратная реализация предложенных генераторов псевдослучайных последовательностей и продемонстрировано ее превосходство над существующими аналогами как по быстрдействию, так и по эффективности.

Методы исследований. Теоретические методы исследований включали применение теории конечных автоматов, теории графов, теории вероятности; эмпирические — проведение компьютерного моделирования и применение методов математической статистики для оценки свойств двоичных последовательностей. Для программной реализации был использован язык C# и платформа Microsoft .NET; разработка аппаратной реализации осуществлялась на языке описания цифровых схем VHDL, в качестве аппаратной платформы применялась ПЛИС Altera Cyclone II.

Достоверность результатов. Достоверность теоретических результатов обеспечивается строгим математическим обоснованием утверждений и подкрепляется их согласованностью с данными компьютерного моделирования. Достоверность эмпирических результатов достигается за счет применения стандартных общепринятых инструментов статистического анализа. Корректность аппаратной реализации подтверждается соответствием ее выходных последовательностей и последовательностей, полученных при помощи программной реализации.

Научная новизна. Научная новизна работы заключается в следующем:

- исследовано влияние веса локальной функции связи на распределение значений ячеек памяти клеточных автоматов; сформулирован, доказан и подтвержден экспериментально критерий сохранения равномерности распределения;

- впервые сформулировано понятие лавинного эффекта для клеточных автоматов; получено теоретическое описание характеристик оптимального лавинного эффекта и эмпирические зависимости характеристик лавинного эффекта от выбора окрестностей ячеек; показано, что клеточные автоматы обладают свойством размножения изменений;
- впервые введено и исследовано понятие пространственного периода в классических клеточных автоматах; сформулировано и доказано необходимое условие существования пространственного периода; показано, что нетривиальный пространственный период существенно снижает верхнюю границу периода последовательности внутренних состояний;
- разработаны новые методы генерации псевдослучайных последовательностей; на основании свойств клеточных автоматов осуществлен синтез структуры генератора и обоснован выбор его параметров; эмпирически подтверждено соответствие статистических свойств выходных последовательностей современным требованиям.

Практическая ценность. Практическая ценность исследований обусловлена превосходством разработанных генераторов над существующими аналогами как по быстродействию, так и по эффективности реализации. Полученные результаты могут быть использованы в широком спектре различных областей, включая имитационное моделирование, численное решение математических задач методами Монте-Карло, криптографическую защиту информации и др. Внедрение предложенных генераторов в прикладные системы позволит увеличить их быстродействие, а также повысить эффективность за счет хороших статистических свойств и контролируемого периода вырабатываемых псевдослучайных последовательностей.

Положения, выносимые на защиту. На защиту выносятся следующие основные положения и результаты диссертационного исследования:

- критерий сохранения равномерности распределения значений ячеек памяти клеточных автоматов;
- понятие лавинного эффекта в клеточных автоматах и его характеристики; законы, описывающие характеристики оптимального лавинного эффекта для классических и неоднородных клеточных автоматов;
- понятие пространственного периода в классических клеточных автоматах и необходимое условие его существования;
- разработанная структура и параметры генераторов псевдослучайных последовательностей на основе клеточных автоматов; обоснование периода выходной последовательности генераторов;
- результаты экспериментального исследования статистических свойств выходных последовательностей предложенных генераторов;
- разработанная аппаратная реализация генераторов псевдослучайных последовательностей и ее характеристики в сравнении с существующими аналогами.

Публикации. Результаты исследований опубликованы в тринадцати научных работах, из них шесть — в изданиях, рекомендованных ВАК Минобрнауки РФ. Все публикации без соавторов.

Апробация. Основные результаты исследований докладывались и обсуждались на 9-ой (2007 г.) и 12-ой (2010 г.) ежегодных международных конференциях РусКрипто (г. Москва), научно-исследовательском семинаре «Защита информации: аспекты теории и вопросы практических приложений» МГТУ им. Н.Э. Баумана (г. Москва, 2010 г.), 9-ой сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» (г. Тюмень, 2010 г.), всероссийской научно-технической конференции «Безопасные информационные технологии» (г. Москва, 2010 г.), научном семинаре кафедры Криптологии и дискретной математики НИЯУ «МИФИ» (г. Москва, 2011 г.).

Результаты исследований внедрены в учебный процесс кафедры «Информационная безопасность» Московского государственного технического университета им. Н.Э. Баумана и кафедры «Комплексная защита информации» Омского государственного технического университета, а также использованы в научно-производственной деятельности ЗАО «Научно-производственное предприятие «Безопасные информационные технологии».

Структура и объем работы. Рукопись диссертации состоит из введения, пяти глав, заключения и шести приложений. Диссертация изложена на 221 странице (из них основная часть — 155 страниц, приложения — 49 страниц), содержит 34 иллюстрации и 18 таблиц. Библиографический список включает 85 наименований.

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Пусть $M = [m_0, m_1, \dots, m_{X-1}]$ — множество двоичных ячеек памяти. Сопоставим каждой ячейке $m_x \in M$ ее *окрестность* — упорядоченный набор $\Psi(m_x) = [m_{x_1}, m_{x_2}, \dots, m_{x_k}]$, мощность которого не зависит от выбора ячейки m_x ; окрестностью Ψ также будем называть правило, по которому каждой ячейке m_x сопоставляется набор $\Psi(m_x)$. Обозначим через $m_x^{(t)}$ значение ячейки m_x в момент времени t , а через $\Psi^{(t)}(m_x)$ — набор, составленный из значений ячеек, входящих в окрестность m_x , в момент времени t .

Неоднородным клеточным автоматом (НКЛА) размера X с окрестностью Ψ и *локальной функцией связи* (ЛФС) f будем называть автономный конечный автомат, состояние которого определяется совокупностью значений ячеек из множества M ($|M| = X$). Временная шкала такого автомата дискретна, а смена значений всех ячеек происходит синхронно при увеличении номера такта в соответствии с зависимостью $m_x^{(t+1)} = f(\Psi^{(t)}(m_x))$, где f является булевой функцией от k переменных (k — мощность окрестности) и не зависит от выбора ячейки m_x .

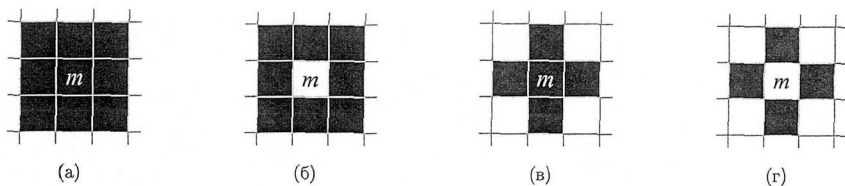


Рис. 1. Типы окрестности двумерных классических клеточных автоматов: (а) и (б) — полная и неполная окрестности Мура, (в) и (г) — полная и неполная окрестности фон Неймана

Классические клеточные автоматы (ККЛА) могут рассматриваться как частный случай неоднородных. В ККЛА множество M упорядочено геометрически: ячейки располагаются в узлах n -мерной прямоугольной решетки размера $X_1 \times X_2 \times \dots \times X_n$. Противоположные края решетки отождествляются, т. е. все действия над координатами выполняются по модулю соответствующего линейного размера решетки. Для обозначения ячейки с координатами (x_1, x_2, \dots, x_n) далее используется запись m_{x_1, x_2, \dots, x_n} .

Расстояние между ячейками $m = m_{x_1, x_2, \dots, x_n}$ и $m^* = m_{x_1^*, x_2^*, \dots, x_n^*}$ ККЛА равно наибольшей по абсолютному значению разности одноименных координат с учетом отождествления краев решетки: $d(m, m^*) = \max_{1 \leq i \leq n} \{\min(|x_i - x_i^*|, X_i - |x_i - x_i^*|)\}$. Максимально возможное расстояние между ячейками классического клеточного автомата составляет $d_{\max} = \max_{m, m^* \in M} \{d(m, m^*)\} = \max_{1 \leq i \leq n} \{[(X_i - 1)/2]\}$.

В окрестность ячейки ККЛА входит подмножество ячеек, удаленных от нее на расстояние не более заданного радиуса локальности r . Все ячейки в ККЛА неразличимы по своим свойствам, поэтому способ формирования окрестности не зависит от выбора ячейки и является характеристикой автомата.

При рассмотрении ККЛА в диссертации основное внимание уделено двумерному случаю с радиусом локальности $r = 1$ как наиболее эффективному с точки зрения аппаратной реализации. Варианты выбора окрестностей ячеек для таких автоматов приведены на рис. 1.

СОДЕРЖАНИЕ РАБОТЫ

Введение. Введение содержит краткий исторический обзор предметной области, постановку целей и задач диссертационной работы, обоснование актуальности исследований, а также общие сведения о структуре и содержании диссертации.

Глава 1. В первой главе приведено формальное понятие генератора псевдослучайных последовательностей и выполнен аналитический обзор су-

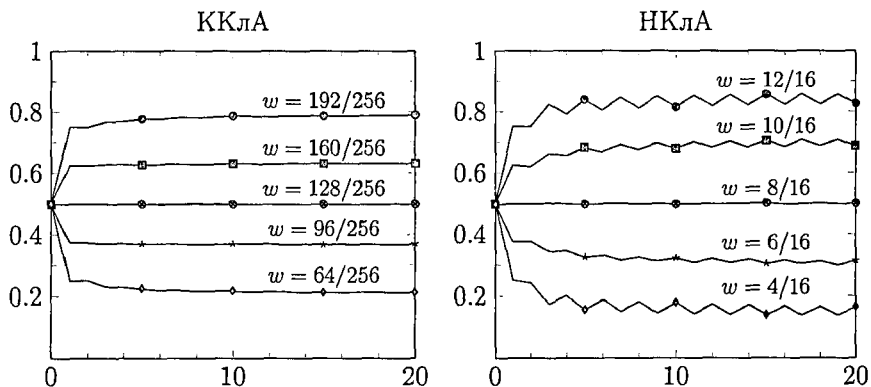


Рис. 2. Эмпирическая зависимость вероятности $\Pr[m^{(t)} = 1]$ от номера такта t при равномерном начальном распределении значений ячеек для различных вариантов нормированного веса w ЛФС

существующих наиболее распространенных генераторов, их достоинств, недостатков, а также методов улучшения свойств. В состав рассмотренных классов генераторов входят линейные и нелинейные конгруэнтные генераторы, генераторы Фибоначчи, генераторы на основе регистров сдвига и генераторы на основе одномерных классических клеточных автоматов. По результатам обзора сделан вывод о том, что существующие генераторы не полностью удовлетворяют современным требованиям.

Глава 2. Во второй главе формализованы понятия НКЛА и ККЛА и исследован ряд свойств, имеющих важное значение при построении генераторов псевдослучайных последовательностей на основе клеточных автоматов: зависимость распределения значений ячеек от веса ЛФС, лавинный эффект и его характеристики, периодичность в клеточных автоматах.

Распределение значений ячеек. В диссертации доказано, что равномерность ЛФС является необходимым и достаточным условием сохранения равномерности распределения значений ячеек в классических клеточных автоматах и неоднородных клеточных автоматах со случайно и равномерно выбранными окрестностями ячеек, что также подтверждается данными компьютерного моделирования (рис. 2).

В силу доказанного критерия при построении генераторов псевдослучайных равномерно распределенных последовательностей следует ограничиться применением клеточных автоматов с равновесными ЛФС.

Лавинный эффект. Лавинный эффект (ЛЭ) был введен Х. Фейстелем для оценки свойств блочных шифров: «хорошим» считается такой ЛЭ, при котором малые изменения входных данных приводят к значительным изме-

нениям выходных. Понятие лавинного эффекта применительно к клеточным автоматам в диссертации использовано впервые.

Лавинный эффект в клеточных автоматах — это изменения в значениях ячеек памяти, возникающие в процессе функционирования клеточного автомата вследствие смены значения одной ячейки в начальный момент времени. В работе введено понятие *оптимального лавинного эффекта*, при котором изменения распространяются с максимально возможной скоростью, причем изменяются значения в среднем половины ячеек, что соответствует классическому лавинному критерию.

При исследовании лавинного эффекта рассматривалась модель, состоящая из двух идентичных клеточных автоматов, различающихся только значением одной ячейки в начальный момент времени. С целью количественного описания ЛЭ в диссертации предложены две числовые характеристики: интегральная и пространственная.

Интегральная характеристика $\eta(t)$ лавинного эффекта отражает временную зависимость отношения количества изменившихся ячеек к размеру клеточного автомата.

Теоретическими методами в работе получено выражение, описывающее интегральную характеристику $\eta_{opt}(t)$ оптимального ЛЭ в классических клеточных автоматах, которое для частного случая двумерных ККЛА с размером решетки $X \times Y$ ($X \geq Y$) и радиусом локальности $r = 1$ имеет вид

$$\eta_{opt}(t) = \begin{cases} (2t+1)^2/(2 \cdot X \cdot Y), & 2t+1 \leq Y, \\ (2t+1)/(2 \cdot X), & Y < 2t+1 \leq X, \\ 1/2, & X < 2t+1. \end{cases}$$

Для НКЛА в диссертации доказано, что если каждая ячейка входит в окрестность ровно k других ячеек, где k — мощность окрестности, то интегральная характеристика оптимального ЛЭ ограничена сверху соотношением

$$\eta_{opt}(t) \leq \begin{cases} \frac{1}{2X} \frac{k^{t+1} - 1}{k - 1}, & (k^{t+1} - 1)/(k - 1) \leq X, \\ 1/2, & (k^{t+1} - 1)/(k - 1) > X, \end{cases}$$

где X — размер клеточного автомата.

Пространственная характеристика $\mu(t)$ лавинного эффекта вводится только для классических клеточных автоматов и равна отношению максимального расстояния, на котором проявились изменения, к максимально возможному расстоянию между ячейками. Таким образом, пространственная характеристика отражает линейную скорость распространения изменений по решетке ККЛА.

В диссертации получено выражение, описывающее пространственную характеристику $\mu_{opt}(t)$ оптимального ЛЭ, для двумерных клеточных автоматов с размером решетки $X \times Y$ ($X \geq Y$) и единичным радиусом локальности

имеющее вид

$$\mu_{opt}(t) = \begin{cases} \frac{t}{\lceil (X-1)/2 \rceil}, & t \leq \lceil (X-1)/2 \rceil, \\ 1, & t > \lceil (X-1)/2 \rceil. \end{cases}$$

По результатам анализа эмпирических данных (рис. 3 и 4) сделан вывод о том, что клеточные автоматы обладают свойством размножения изменений, причем характеристики лавинного эффекта улучшаются с увеличением мощности окрестности, и для ККЛА с окрестностями Мура практически совпадают с таковыми для оптимального ЛЭ. Кроме того, при фиксированной мощности окрестности лавинный эффект в НКЛА выражен более ярко по сравнению с ККЛА.

Периодичность. Период последовательности внутренних состояний произвольного клеточного автомата размера X ограничен сверху неравенством $T \leq T_{max} = 2^X$, которое при $X \geq 2$ является строгим.

В классических клеточных автоматах возможно формирование *пространственных периодов*, характеризующихся выполнением равенства $m_{x_1, \dots, x_i, \dots, x_n}^{(t)} = m_{x_1+k_1T_1, \dots, x_i+k_iT_i, \dots, x_n+k_nT_n}^{(t)}$ для всех ячеек ККЛА при любых целых k_i (действия над координатами ячеек выполняются по модулю соответствующего линейного размера решетки). T_i — наименьшее целое число, при котором равенство верно — является величиной пространственного периода вдоль оси X_i .

Существование пространственного периода позволяет рассматривать вместо исходного ККЛА с решеткой размера $X_1 \times X_2 \times \dots \times X_n$ клеточный автомат с решеткой размера $T_1 \times T_2 \times \dots \times T_n$ и приводит к уменьшению максимально возможного периода последовательности внутренних состояний в $2^{X_1 \cdot X_2 \cdot \dots \cdot X_n - T_1 \cdot T_2 \cdot \dots \cdot T_n}$ раз, что недопустимо при использовании клеточных автоматов в структуре генераторов псевдослучайных последовательностей.

В диссертации доказано, что необходимым условием существования пространственного периода является делимость линейных размеров решетки X_i на соответствующие величины пространственных периодов T_i . Исходя из доказанного условия сделан вывод о том, что для исключения возникновения нетривиальных пространственных периодов в классических клеточных автоматах в качестве размеров решетки следует выбирать простые числа.

Глава 3. В третьей главе осуществлен синтез структуры и обоснован выбор параметров генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов.

Генератор включает два клеточных автомата C_1 и C_2 и регистр сдвига с линейными обратными связями R (рис. 5). На каждом такте работы клеточные автоматы вырабатывают по 256 бит первичных псевдослучайных последовательностей. Выходная последовательность генератора формируется посредством поэлементного сложения по модулю 2 первичных последо-

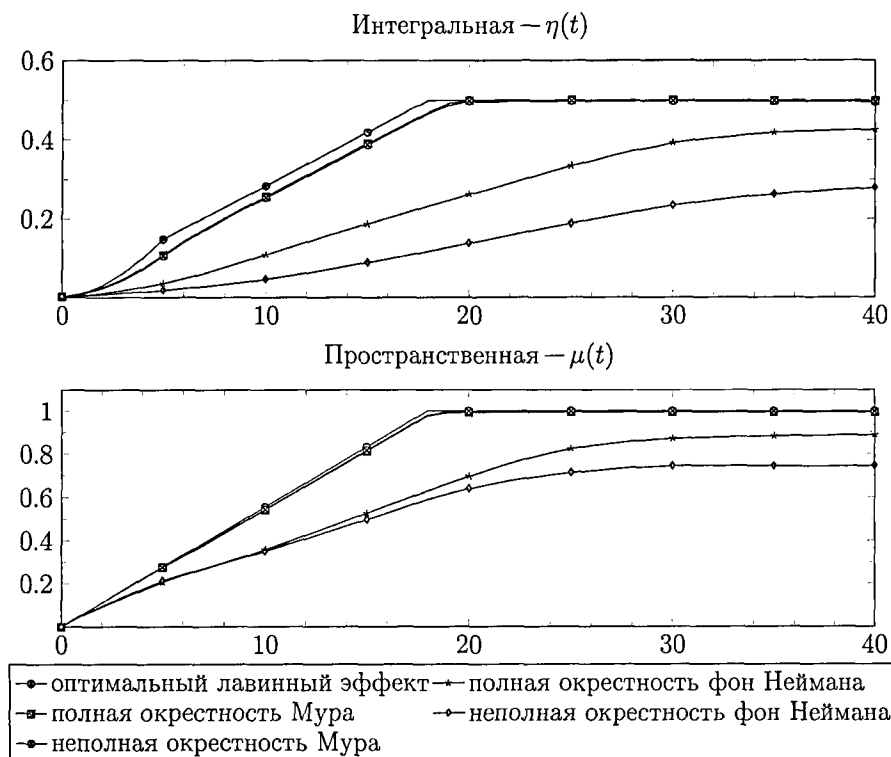


Рис. 3. Усредненные эмпирические характеристики ЛЭ в ККЛА для различных вариантов выбора окрестности

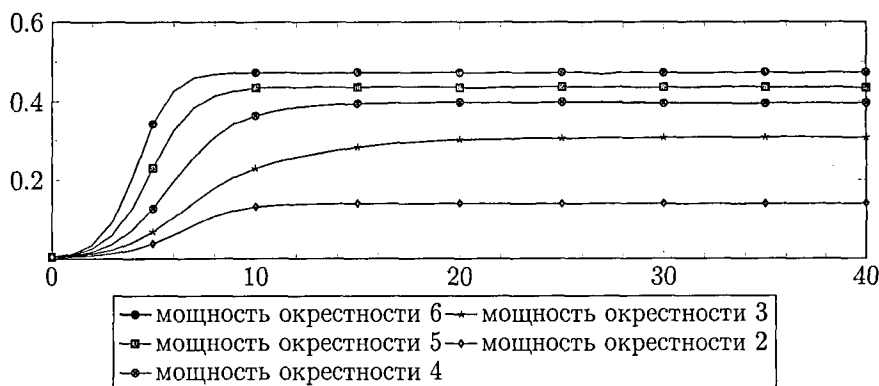


Рис. 4. Усредненная эмпирическая интегральная характеристика $\eta(t)$ ЛЭ в НКЛА при различных вариантах мощности окрестности

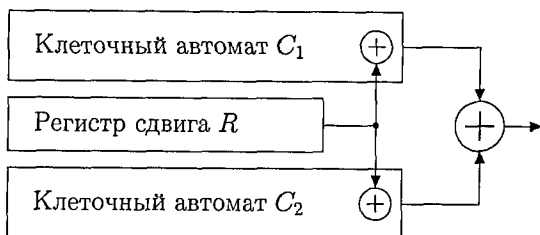


Рис. 5. Структура генератора

вательностей, что позволяет обеспечить хорошие статистические свойства, а также затруднить восстановление внутреннего состояния генератора по его выходу.

В состав генератора на основе классических клеточных автоматов в качестве C_1 и C_2 входят двумерные ККЛА размера 37×11 ячеек с неполной окрестностью Мура. Использование простых чисел в качестве размеров решетки исключает формирование пространственных периодов, а выбор окрестности обусловлен соответствующими ей хорошими характеристиками лавинного эффекта. Выход каждого клеточного автомата формируется из значений ячеек, лежащих на подрешетке размера 32×8 .

При построении генератора на основе неоднородных клеточных автоматов их размер составляет 257 ячеек. Мощность окрестности равна 4, что позволяет достичь компромисса между характеристиками лавинного эффекта и эффективностью аппаратной реализации, а сама окрестность выбирается случайным образом для каждой ячейки. Выход автоматов формируется из значений ячеек с индексами от 0 до 255.

В обоих случаях начальные значения ячеек памяти клеточных автоматов являются фиксированными и соответствуют равномерному распределению, а в качестве локальной функции связи используется равновесная булева функция, что позволяет обеспечить равномерность распределения значений ячеек в процессе функционирования генератора.

Регистр сдвига с линейными обратными связями R используется для контроля периода выходной последовательности генератора. Выход регистра прибавляется по модулю 2 к значению одной из ячеек каждого клеточного автомата (для ККЛА — с координатами (34, 9), для НКЛА — с индексом 256), не используемых напрямую при формировании первичных выходных последовательностей. Свойство размножения изменений в клеточных автоматах позволяет утверждать, что период выходной последовательности генератора будет не менее периода выходной последовательности регистра сдвига.

В диссертации использован регистр длины 63, для которого нижняя оценка периода выходной последовательности генератора составляет

$T \geq 256 \cdot (2^{63} - 1) \approx 2,36 \cdot 10^{21}$. При необходимости обеспечения большего периода длина регистра может быть увеличена.

Начальные значения ячеек памяти регистра сдвига являются переменными и играют роль *вектора инициализации* генератора, обеспечивая выбор конкретной выходной последовательности из множества возможных.

Функционирование генератора включает три фазы:

- 1) фазу *инициализации*, на которой в ячейки памяти регистра сдвига заносятся начальные значения;
- 2) фазу *холостого хода*, необходимую для распространения влияния выхода регистра сдвига на все ячейки клеточного автомата за счет лавинного эффекта;
- 3) фазу *генерации*, в процессе которой вырабатывается выходная последовательность.

Глава 4. Четвертая глава посвящена описанию методики и результатов исследования статистических свойств выходных последовательностей разработанных генераторов.

В качестве инструмента исследования применялся общепризнанный в мировой практике набор статистических тестов Национального института стандартов и технологии США (NIST). В состав набора входят 15 разновидностей проверок, направленных на выявление статистических отклонений выходных последовательностей генераторов от случайных равномерно распределенных двоичных последовательностей.

Исследование проводилось по итеративной схеме в четыре этапа, различающихся составом проверок, количеством и длиной выходных последовательностей каждого генератора. В каждый следующий этап включались только генераторы, показавшие наилучшие результаты на предыдущем, что значительно сократило требования к вычислительным ресурсам. Параметры последнего — четвертого — этапа исследований выбирались в полном соответствии с рекомендациями NIST.

В рамках диссертационной работы был разработан программный комплекс автоматизации процесса тестирования, осуществляющий формирование входных данных и обработку результатов в пакетном режиме.

Всего было исследовано по 10 000 генераторов на основе ККЛА и НКЛА. В процессе исследования определены конкретные локальные функции связи и, для НКЛА, окрестности ячеек клеточных автоматов, при которых разработанные генераторы успешно проходят весь набор статистических тестов.

Глава 5. В пятой главе описывается аппаратная реализация разработанных генераторов и проводится ее сравнение с современными аналогами.

Описание реализации. В качестве платформы для аппаратной реализации используется недорогая ПЛИС (FPGA) Altera Cyclone II. Выходная последовательность генератора по 256-разрядной шине подается напрямую

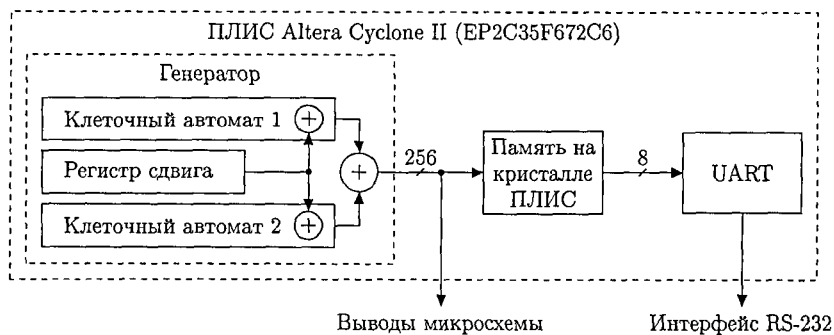


Рис. 6. Структурная схема аппаратной реализации

на выходы микросхемы, а также записывается во внутреннюю память ПЛИС для дальнейшего анализа (рис. 6).

Номинальная тактовая частота работы схемы составляет 100 МГц, причем статический анализ временных задержек показал, что она может быть увеличена до 140 МГц при построении генераторов на основе классических и до 149 МГц — на основе неоднородных клеточных автоматов без внесения каких-либо изменений в аппаратную реализацию.

Структура клеточных автоматов позволяет вычислять новые значения всех ячеек параллельно, что обеспечивает высокую эффективность аппаратной реализации генератора и формирование 256 бит выхода за один такт синхронизации схемы. Таким образом, скорость выработки псевдослучайной последовательности на номинальной тактовой частоте составляет 23,8 Гбит/с.

Разработка осуществлялась в САПР Altera Quartus II на языке описания цифровых устройств VHDL.

Сравнительные характеристики. Сравнение быстродействия и эффективности аппаратной реализации проводилось с генераторами, представленными на европейский конкурс eSTREAM.

В качестве показателя быстродействия использовалась скорость выработки выходной последовательности на максимальной тактовой частоте и на частоте 100 МГц. Нормирование по частоте обусловлено применением технологии специализированных микросхем ASIC для реализации генераторов, представленных на конкурс eSTREAM. Технология ASIC обеспечивает функционирование на более высокой по сравнению с FPGA тактовой частоте, однако требует существенно больших финансовых и технологических затрат. Как видно из графиков на рис. 7, по быстродействию разработанная аппаратная реализация превосходит лучший из аналогов — алгоритм Trivium — на максимальной тактовой частоте в два, на частоте 100 МГц — в четыре раза.

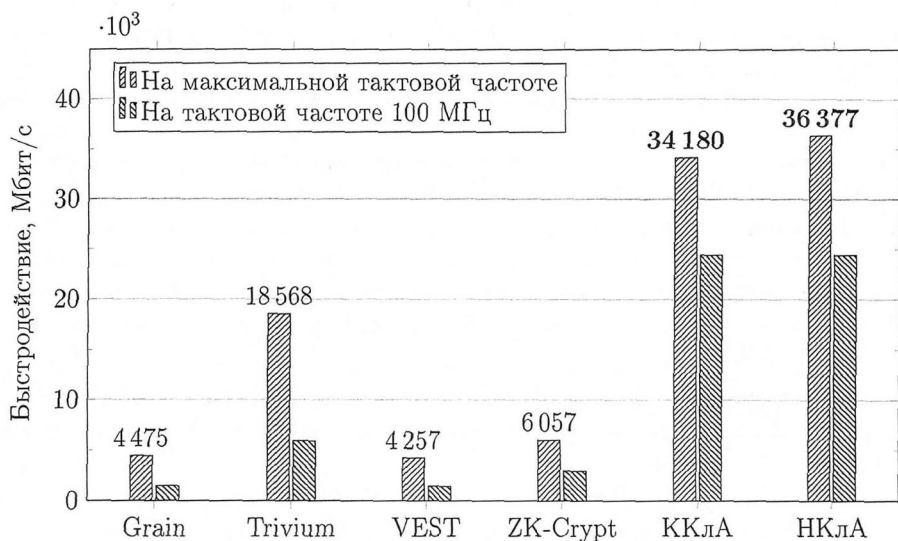


Рис. 7. Сравнение быстродействия разработанной аппаратной реализации и генераторов, представленных на конкурс eSTREAM

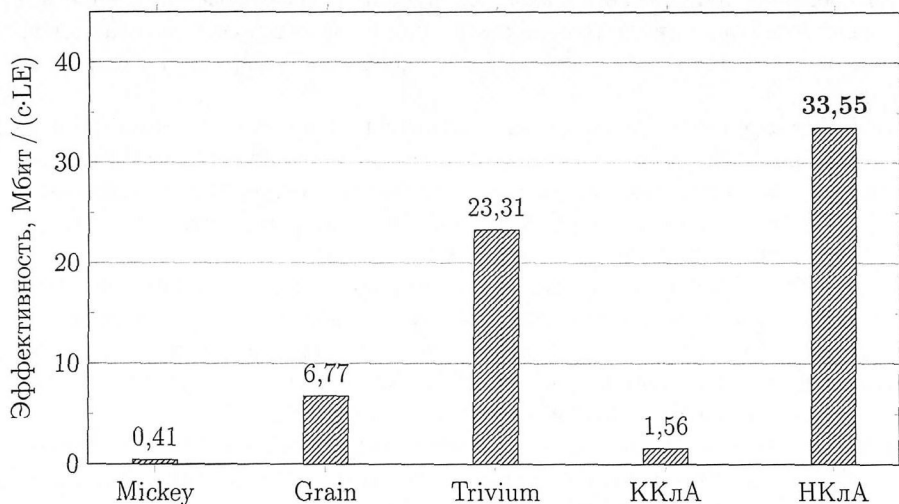


Рис. 8. Сравнение эффективности разработанной аппаратной реализации и генераторов, представленных на конкурс eSTREAM

В качестве показателя эффективности было выбрано отношение скорость выработки выходной последовательности на максимальной тактовой частоте к количеству использованных аппаратных ресурсов (для ПЛИС Altera единицей ресурсов является логический элемент — LE). Сравнение показало (рис. 8), что наибольшей эффективностью, значительно превосходящей аналоги, обладает реализация генератора на основе неоднородных клеточных автоматов, что объясняется малой мощностью окрестности. Эффективность реализации генератора на основе классических клеточных автоматов является сравнительно невысокой, однако может быть существенно улучшена за счет использования старших семейств ПЛИС, таких как Altera Stratix, позволяющих реализовать булеву функцию от 8 переменных в пределах одного LE.

Заключение. В заключении приведены основные результаты диссертационной работы и обозначены возможные направления дальнейших исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

- 1) Проведен аналитический обзор наиболее распространенных генераторов псевдослучайных последовательностей, выявлены их основные достоинства и недостатки; рассмотрены методы улучшения статистических свойств выходных последовательностей.
- 2) Исследовано влияние веса локальной функции связи на распределение значений ячеек памяти клеточных автоматов; сформулирован, доказан и подтвержден эмпирически критерий сохранения равномерности распределения.
- 3) Впервые сформулировано понятие лавинного эффекта в клеточных автоматах; получено теоретическое описание характеристик оптимального лавинного эффекта и эмпирические зависимости характеристик лавинного эффекта от выбора окрестностей ячеек; показано, что клеточные автоматы обладают свойством размножения изменений.
- 4) Впервые введено и исследовано понятие пространственного периода в классических клеточных автоматах; сформулировано и доказано необходимое условие существования пространственного периода; показано, что нетривиальный пространственный период существенно снижает верхнюю границу периода последовательности внутренних состояний.
- 5) Разработаны новые методы генерации псевдослучайных последовательностей; осуществлен синтез структуры генератора и обоснован выбор его параметров; указан способ обеспечения заданного периода выходной последовательности; разработана эталонная программная реализация генераторов на языке высокого уровня C#.

- 6) Исследованы статистические свойства выходных последовательностей разработанных генераторов; определены конкретные локальные функции связи и окрестности ячеек клеточных автоматов, обеспечивающие хорошие статистические свойства выходных последовательностей; подтверждено соответствие статистических свойств современным требованиям; разработан программный комплекс автоматизации процесса статистического тестирования.
- 7) Разработана и изготовлена в виде устройства на ПЛИС высокоскоростная аппаратная реализация предложенных генераторов, превосходящая аналоги как по быстродействию, так и по эффективности.

ПУБЛИКАЦИЯ РЕЗУЛЬТАТОВ ДИССЕРТАЦИИ

- 1) Сухинин Б. М. Применение клеточных автоматов в криптографии // Интеллектуальные системы: Труды Восьмого международного симпозиума / Под ред. К. А. Пупкова. М., 2008. С. 509 – 512.
- 2) Сухинин Б. М. Применение классических и неоднородных клеточных автоматов при построении высокоскоростных генераторов псевдослучайных последовательностей // Проектирование и технология электронных средств. 2009. № 3. С. 47 – 51.
- 3) Сухинин Б. М. О влиянии параметров локальной функции связи на распределение значений ячеек двоичных клеточных автоматов // Объединенный научный журнал. 2010. № 8. С. 39 – 41.
- 4) Сухинин Б. М. О лавинном эффекте в клеточных автоматах // Объединенный научный журнал. 2010. № 8. С. 41 – 46.
- 5) Сухинин Б. М. О новом классе генераторов псевдослучайных последовательностей на основе клеточных автоматов // Объединенный научный журнал. 2010. № 8. С. 46 – 49.
- 6) Сухинин Б. М. Практические аспекты оценки качества генераторов случайных последовательностей с равномерным распределением // Объединенный научный журнал. 2010. № 8. С. 49 – 55.
- 7) Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. № 2. С. 34 – 41.
- 8) Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. Приложение № 3. С. 32 – 34.
- 9) Сухинин Б. М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование: электронное научно-техническое издание. 2010. № 8. URL: <http://technomag.edu.ru/doc/159565.html> (дата обращения: 01.10.2010).
- 10) Сухинин Б. М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и об-

- разование: электронное научно-техническое издание. 2010. №9. URL: <http://technomag.edu.ru/doc/159714.html> (дата обращения: 01.10.2010).
- 11) Сухинин Б. М. Генераторы псевдослучайных последовательностей на основе клеточных автоматов // Безопасные информационные технологии. Сборник тезисов докладов всероссийской научно-технической конференции (выпуск второй) / Под ред. В. А. Матвеева. М., 2011. С. 14 – 17.
 - 12) Сухинин Б. М. О некоторых свойствах клеточных автоматов и их применении в структуре генераторов псевдослучайных последовательностей // Вестник МГТУ. Приборостроение. 2011. № 2. С. 68 – 76.
 - 13) Сухинин Б. М. Однородные двумерные булевы клеточные автоматы и их свойства применительно к генерации псевдослучайных последовательностей // Системы высокой доступности. 2011. Т. 7, № 2. С. 39 – 41.

Подписано к печати 28.10.11. Заказ № 738
Объем 1,0 печ.л. Тираж 100 экз.
Типография МГТУ им. Н.Э. Баумана
105005, Москва, 2-я Бауманская ул., д.5
(499) 263-62-01