электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0420900025. ISSN 1994-0408

Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов

№ 09, сентябрь 2010 г.

Автор: Б. М. Сухинин

УДК 004.421.5

МГТУ им. Н. Э. Баумана, Россия, г. Москва

E-mail: b.sukhinin@gmail.com

Генерация случайных чисел слишком важна, чтобы оставлять ее на волю случая.

Р. Кавью, ORNL

Введение

Последовательности случайных чисел широко используются в самых разных приложениях — от компьютерного программирования, имитационного моделирования и методов Монте-Карло до криптографии. При этом от свойств случайных последовательностей напрямую зависит качество получаемых результатов.

Выделяют два основных класса генераторов случайных последовательностей [1]:

– генераторы *истинно случайных* последовательностей;

– генераторы *псевдослучайных* последовательностей.

Генераторы истинно случайных последовательностей основываются на различных физических процессах и явлениях, имеющих случайную природу. До начала XX в. такие последовательности имитировались при помощи простейших случайных экспериментов: бросания монеты или игральной кости, вытягивания шаров из урны, раскладывания карт и т. д. В 1927 г. английским ученым Леонардом Типпетом были опубликованы таблицы [2],

содержащие свыше 40 000 случайных цифр, «произвольно извлеченных из отчетов о переписи населения».

Позже были разработаны механические генераторы случайных чисел. Первая подобная машина была использована в 1939 г. Кендаллом и Бабингтон-Смитом для построения таблицы [3], содержащей 100 000 случайных чисел. Компьютер Ferranti Mark I, запущенный в 1951 г., обладал встроенным резисторным генератором шума, 20 бит с которого при помощи специальной программы подавались на сумматор (этот метод был предложен Аланом Тьюрингом). В 1955 г. RAND Corporation опубликовала таблицы [4], в которых содержался миллион случайных чисел, полученных при помощи специально сконструированной ЭВМ.

В настоящее время спрос на генераторы случайных последовательностей с заданными вероятностными распределениями, а также на сами случайные последовательности настолько возрос, что за рубежом стали появляться научно-производственные фирмы, специализирующиеся на подготовке больших массивов случайных чисел. Например, с 1996 г. распространяется компакт-диск «The Marsaglia Random Number CDROM» [5], который содержит 4,8 млрд. «истинно случайных» бит, а в сети Интернет можно найти массивы случайных чисел, полученные в результате измерения атмосферных шумов (Random.Org, [6]) или регистрации радиоактивного распада (HotBits, [7]).

Подобные методы дают очень хорошие статистические результаты, но требуют колоссального времени для получения последовательностей необходимой на практике длины. Так, быстродействие генератора HotBits составляет всего около 100 байт в секунду. Поэтому после изобретения компьютеров начались интенсивные поиски эффективных программных способов генерации случайных чисел.

Поскольку любая программа реализует некоторый детерминированный алгоритм, получить истинно случайные числа только с ее помощью невозможно. В связи с этим Джон фон Нейман отмечал, что «каждый, кто использует арифметические методы генерации случайных чисел, безусловно, грешит». Тем не менее, подобные генераторы позволяют строить последовательности, схожие (в идеальном случае — неотличимые) с истинно случайными по своим свойствам, и потому носят название генераторов псевдослучайных

последовательностей.

Практически все алгоритмы генерации псевдослучайных последовательностей обладают в той или иной мере различными недостатками, такими как слишком короткий период выходной последовательности, наличие корреляции между различными ее членами, неравномерное распределение, предсказуемость, недостаточная скорость, сложность реализации и т. д. Поэтому актуальной научной и инженерной задачей является разработка новых генераторов, сочетающих в себе высокое быстродействие и хорошие статистические свойства формируемой псевдослучайной последовательности.

1. Постановка задачи

Случайной равномерно распределенной двоичной последовательностью называется бесконечная последовательность вида

$$\alpha_1, \alpha_2, \ldots, \quad \alpha_i \in \{0; 1\}.$$

Такая последовательность удовлетворяет следующим двум фундаментальным свойствам:

- для любого числа $n \in \mathbb{N}$ и произвольных значений индексов $1 \leqslant i_1 < i_2 < \ldots < i_n$ случайные величины $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}$ независимы в совокупности;
- для любого индекса $i \in \mathbb{N}$ случайная величина α_i имеет равномерное на множестве $\{0; 1\}$ распределение вероятностей, т. е. $\Pr[\alpha_i = 0] = \Pr[\alpha_i = 1] = 1/2$.

Отметим, что задача генерации случайной двоичной последовательности с заданным законом распределения может быть сведена [8] при помощи известных методов обратной функции, исключения и композиции к генерации случайной равномерно распределенной двоичной последовательности.

Целью исследования является разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов, отвечающих следующим требованиям:

- выходные последовательности алгоритмов должны обладать доказуемо большим периодом, существенно превосходящим требуемое на практике количество членов;
- выходные последовательности алгоритмов должны быть статистически неотличимы-

ми от случайных равномерно распределенных двоичных последовательностей, что должно подтверждаться успешным прохождением специализированных наборов статистических тестов;

– реализация алгоритмов должна обладать высоким быстродействием;
– эффективность реализации не должна быть ниже, чем у существующих аналогов при тех же параметрах быстродействия.

2. Краткие сведения о клеточных автоматах

В общем виде *клеточный автомат* представляет собой набор ячеек памяти, способных хранить значения из некоторого конечного множества. Для каждой ячейки выбирается множество связанных с ней ячеек того же клеточного автомата — т. н. *окрестность*. Время клеточного автомата изменяется дискретными шагами (тактами). Смена значений всех ячеек происходит синхронно в момент увеличения номера такта. Значение каждой ячейки на следующем такте определяется в соответствии с *правилами переходов* в зависимости от текущих значений ячеек, входящих в ее окрестность.

В *классических клеточных автоматах* [9, 10] набор ячеек представляется в виде упорядоченного множества, элементы которого располагаются в узлах n-мерной решетки (наибольшее распространение получили автоматы с одно-, двух- и трехмерными решетками [11]). Кроме того, для классических клеточных автоматов выполняются свойства *однородности* и *локальности*. Однородность означает, что все ячейки клеточного автомата являются неразличимыми по своим свойствам: для них используются одни и те же правила переходов и одинаковые способы выбора окрестности, а для решения проблемы граничных клеток противоположные края решетки отождествляются (для двумерных клеточных автоматов это эквивалентно «закручиванию» решетки в тор). В соответствии со свойством локальности, в окрестность каждой ячейки входит подмножество ячеек, удаленных от данной на расстояние не более заданного и, возможно, она сама.

Неоднородные клеточные автоматы являются обобщением классического случая: как следует из названия, для таких автоматов свойство однородности может не выполняться. В настоящее время существует несколько различных определений понятия неоднород-

ного клеточного автомата [11–13]. Мы под этим термином будем подразумевать клеточные автоматы, в которых набор ячеек рассматривается в виде неупорядоченного множества, а окрестность выбирается для каждой ячейки произвольным образом; тем не менее, правила переходов и мощность окрестности являются общими для всех ячеек.

В дальнейшем будут рассматриваться только *двоичные клеточные автоматы*, ячейки памяти которых способны хранить значения из множества $\{0; 1\}$, а правила переходов задаются булевой функцией с числом аргументов, равным мощности окрестности.

Выбор параметров клеточных автоматов определяется компромиссом между эффективностью реализации и обеспечением хороших свойств выходной последовательности.

При аппаратной реализации каждая ячейка двоичного клеточного автомата представляется в виде D-триггера и логической таблицы, соответствующей правилам переходов. Сложность реализации таблицы и, соответственно, требуемый объем аппаратных ресурсов напрямую связаны с длиной вектора значений булевой функции переходов, которая, в свою очередь, экспоненциально зависит от мощности окрестности ячейки. Существенным преимуществом аппаратной реализации является параллельное вычисление значений всех ячеек, за счет чего достигается высокое быстродействие схемы.

При программной реализации значения ячеек вычисляются последовательно с использованием общей логической таблицы, и потому длина вектора функции переходов не играет существенной роли. Тем не менее, время вычисления индекса в таблице линейно зависит от количества аргументов функции, т. е. от мощности окрестности ячейки: чем меньше аргументов, тем быстрее может быть вычислен индекс.

В рассматриваемых нами генераторах на выход клеточного автомата подаются значения некоторого подмножества его ячеек. Увеличение числа ячеек памяти позволяет повысить быстродействие аппаратной реализации (за счет параллельности вычислений) ценой линейного увеличения объема требуемых ресурсов. При программной реализации увеличение количества ячеек не оказывает влияния на быстродействие, а возрастание требований к объему памяти является несущественным.

Таким образом, наиболее эффективной реализацией обладают клеточные автоматы с окрестностями небольшой мощности, а количество ячеек памяти должно определяться

требуемым быстродействием. Тем не менее, следует учитывать, что увеличение числа ячеек и уменьшение мощности окрестности оказывает негативное влияние на характеристики лавинного эффекта в клеточных автоматах [14].

3. Структура генератора

В структуру генератора псевдослучайных двоичных последовательностей на основе клеточных автоматов (рис. 1) входят:

– два клеточных автомата C_1 и C_2;

– регистр сдвига с линейными обратными связями R.

Отметим, что генератор может быть построен на основе как классических, так и неоднородных клеточных автоматов.

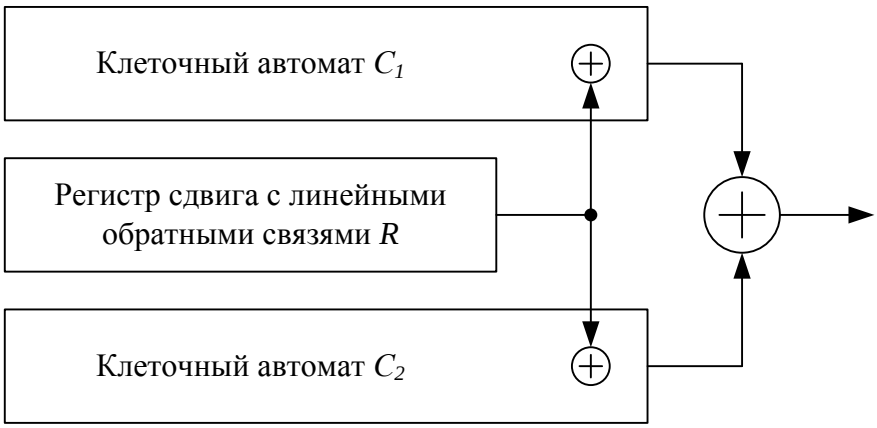

Рис. 1. Структура генератора двоичных псевдослучайных последовательностей на основе клеточных автоматов.

На каждом такте работы клеточные автоматы C_1 и C_2 вырабатывают по 256 бит двоичных последовательностей, которые почленно складываются по модулю 2, а результат сложения подается на выход генератора. Поскольку последовательности, вырабатываемые клеточными автоматами, могут рассматриваться как независимые, сложение позволяет улучшить статистические свойства выходной последовательности генератора [15].

Кроме того, сложение по модулю 2 является одной из двух нетривиальных корреляционно-иммунных булевых функций 1-го порядка от двух переменных (другой такой функцией является его инверсия) [16]. Это означает, что количество информации по Шеннону, содержащееся в значении функции о любом из ее аргументов, равно ну-

лю. Таким образом, сложение выходных последовательностей клеточных автоматов также позволяет затруднить восстановление внутреннего состояния генератора (т. е. значений ячеек памяти клеточных автоматов и регистра сдвига) по выходной последовательности, что может быть полезно, например, в криптографических приложениях.

Одной из основных проблем при использовании клеточных автоматов в составе генераторов псевдослучайных последовательностей является непредсказуемость их периода, обусловленная нелинейностью функции переходов. Для обеспечения минимального гарантированного периода выходной последовательности мы вводим в структуру генератора регистр сдвига с линейными обратными связями R. Выход регистра на каждом такте работы прибавляется по модулю 2 к значению одной из ячеек клеточных автоматов. При этом лавинный эффект позволяет гарантировать, что период последовательности внутренних состояний клеточных автоматов будет не меньше периода выходной последовательности регистра сдвига. Начальные значения ячеек памяти регистра сдвига также являются *ключом* выработки псевдослучайной последовательности генератора в целом, т. е. определяют выбор конкретной последовательности из множества возможных.

4. Особенности построения генератора на основе классических клеточных автоматов

Одномерные клеточные автоматы и возможности их применения в качестве генераторов псевдослучайных последовательностей были исследованы Стефаном Вольфрамом [17–19] и в настоящее время не представляют серьезного интереса. При увеличении размерности решетки мощность окрестности возрастает экспоненциально, и уже для трехмерного случая эффективность реализации клеточных автоматов резко падает.

При построении генератора на основе классических клеточных автоматов мы используем автоматы с двумерной решеткой. В окрестность каждой ячейки входят все ячейки, непосредственно смежные с ней, что соответствует мощности 8. Как было показано в [14], выбор окрестностей меньшей мощности приводит к существенному ухудшению характеристик лавинного эффекта. Увеличение же мощности окрестности ведет к возрастанию числа аргументов функции переходов и делает реализацию автомата неэффективной.

Размер решетки двумерных клеточных автоматов выбран равным 37×11 ячеек. Использование простых чисел в качестве линейных размеров позволяет снизить вероятность возникновения пространственных периодов, поскольку величина такого периода должна делить соответствующий размер решетки. Выходная последовательность автомата формируется из значений ячеек подрешетки размера 32×8 (рис. 2). Выход регистра сдвига с линейными обратными связями прибавляется к ячейке с координатами $(34; 9)$ на каждом такте работы автомата.

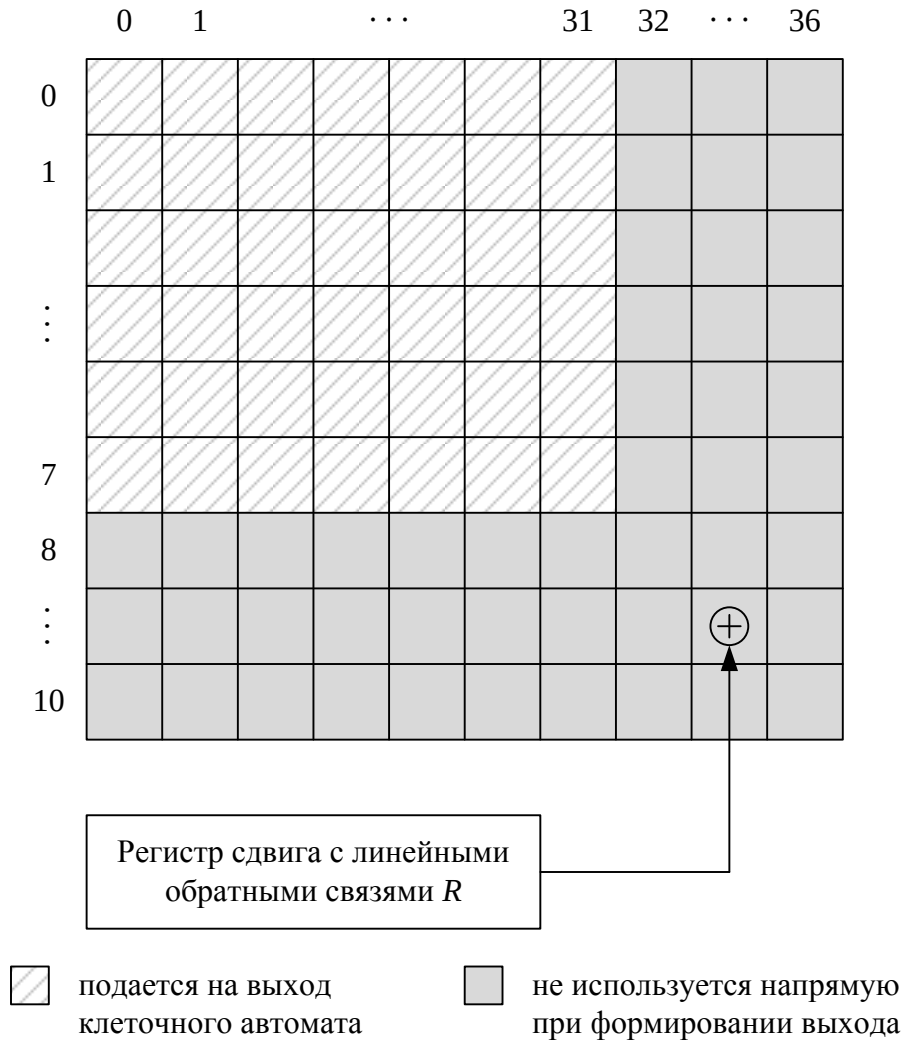

Рис. 2. Особенности использования классических двумерных клеточных автоматов в структуре генератора псевдослучайных последовательностей.

Выбор размера решетки и способа формирования выходной последовательности обеспечивает выработку 256 бит выхода за один такт работы и является, на наш взгляд, оптимальным. При аппаратной реализации увеличение размера решетки и количества вырабатываемой за один такт информации позволяет повысить быстродействие, однако

требует применения шины данных большей разрядности; уменьшение же размера приводит к снижению быстродействия и является неоправданным. При этом на характеристики программной реализации, как было отмечено выше, размер решетки не оказывает существенного влияния.

Использование для формирования выходной последовательности только части ячеек позволяет затруднить полное восстановление внутреннего состояния клеточного автомата (т. е. значений всех ячеек) по его выходу. Из тех же соображений выбрана ячейка для «подмешивания» (сложения по модулю 2) выхода регистра сдвига: она является наиболее удаленной от точек съема информации, и выход регистра никогда в чистом виде не присутствует в выходной последовательности клеточного автомата.

Начальные заполнения (значения ячеек памяти) клеточных автоматов являются фиксированными и рассматриваются как параметр генератора, что позволяет сократить размер ключа выработки последовательности. При этом для клеточных автоматов C_1 и C_2 используются различные начальные заполнения, а значения ячеек подчиняются равномерному закону распределения.

Легко показать [14], что сохранение равномерного распределения значений ячеек памяти в процессе функционирования клеточного автомата достигается только при условии равновесности функции переходов. Кроме того, для повышения линейной сложности выходной последовательности и улучшения ее статистических свойств такая функция должна быть нелинейной. В качестве функций переходов используются равновесные булевы функции, вектор значений которых был получен случайным образом. Возможность применения конкретной функции определяется по результатам исследования статистических свойств выходных последовательностей генератора. Отметим, что автоматам C_1 и C_2 в структуре генератора соответствуют различные функции переходов.

5. Особенности построения генератора на основе неоднородных клеточных автоматов

При использовании неоднородных клеточных автоматов выбор параметров во многом определяется соображениями взаимозаменяемости неоднородных и классических кле-

точных автоматов в структуре генератора.

Каждый клеточный автомат содержит 257 ячеек памяти. Выходная последовательность автомата формируется из значений 256 ячеек, а оставшаяся ячейка используется для «подмешивания» выхода регистра сдвига с линейными обратными связями (рис. 3).

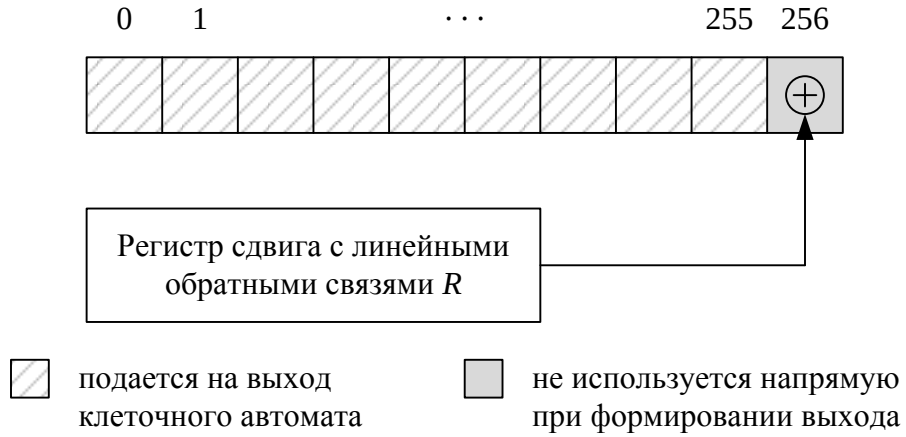

Рис. 3. Особенности использования неоднородных клеточных автоматов в структуре генератора псевдослучайных последовательностей.

Поскольку в неоднородных клеточных автоматах характеристики лавинного эффекта существенно лучше, чем в классических при той же мощности окрестности, используется окрестность мощности 4. Это позволяет существенно снизить сложность и повысить эффективность аппаратной реализации и не оказывает негативного влияния на характеристики программной реализации. Структура связей (т. е. конкретные ячейки, входящие в окрестность данной) выбирается случайным равновероятным образом из всего множества ячеек и является фиксированной для каждого клеточного автомата.

Выбор начальных значений ячеек памяти и функций переходов осуществляется так же, как и в случае классических клеточных автоматов.

6. Алгоритм работы генератора

Алгоритм работы генератора псевдослучайных двоичных последовательностей включает в себя фазы *инициализации* (установки начальных значений), *холостого хода* (функционирования без съема выходной последовательности) и *генерации*:

1. инициализация:

   1.1. присвоить счетчику тактов значение $t = 0$;

1.2. занести ключ выработки последовательности в ячейки памяти регистра сдвига с линейными обратными связями R;

1.3. перейти к шагу 2.1 (фазе холостого хода);

2. холостой ход:

2.1. вычислить новые значения ячеек памяти клеточных автоматов C_1 и C_2 путем применения функции переходов к окрестности каждой ячейки;

2.2. прибавить выходное значение регистра сдвига R к значениям соответствующих ячеек клеточных автоматов C_1 и C_2;

2.3. вычислить новое состояние регистра сдвига R;

2.4. увеличить счетчик тактов t на единицу;

2.5. если $t < T_{idle}$ (T_{idle} — продолжительность фазы холостого хода), перейти к шагу 2.1; иначе перейти к шагу 3.1 (фазе генерации);

3. генерация:

3.1. вычислить новые значения ячеек памяти клеточных автоматов C_1 и C_2 путем применения функции переходов к окрестности каждой ячейки;

3.2. прибавить выходное значение регистра сдвига R к значениям соответствующих ячеек клеточных автоматов C_1 и C_2;

3.3. вычислить новое состояние регистра сдвига R;

3.4. сформировать выходные значения клеточных автоматов C_1 и C_2 из значений подмножеств их ячеек;

3.5. вычислить выходные значения генератора путем сложения по модулю 2 выходных значений клеточных автоматов;

3.6. увеличить счетчик тактов t на единицу;

3.7. если получена выходная последовательность генератора достаточной длины, работа алгоритма завершена; иначе перейти к шагу 3.1;

На фазе инициализации производится загрузка ключа выработки псевдослучайной последовательности в регистр R.

Фаза холостого хода необходима для того, чтобы выход регистра R распространился по ячейкам памяти клеточного автомата (в противном случае на первых тактах работы

выходная последовательность генератора будет определяться только параметрами клеточных автоматов и не будет зависеть от ключа выработки последовательности). Продолжительность фазы холостого хода T_{idle} определяется характеристиками лавинного эффекта. Для выбранных параметров клеточных автоматов мы считаем достаточной величину $T_{idle} = 40$. Тем не менее, поскольку длительность фазы холостого хода мала по сравнению с длительностью фазы генерации, указанная величина может быть увеличена без существенного влияния на производительность алгоритма в целом.

Фаза генерации является основной фазой работы алгоритма и обеспечивает формирование выходной псевдослучайной последовательности. Продолжительность этой фазы определяется требуемой длиной последовательности и зависит от конкретных условий применения генератора.

7. Оценка периода выходной последовательности генератора

При оценке периода выходной последовательности генератор рассматривается как автономный конечный автомат. Состояние такого автомата определяется значениями всех ячеек его внутренней памяти. Если обозначить через M_{C_1} и M_{C_2} размеры клеточных автоматов, а через M_R — длину регистра сдвига, то общее количество ячеек памяти генератора M_G составит

$$M_G = M_{C_1} + M_{C_2} + M_R.$$

Период последовательности внутренних состояний генератора T_G ограничен сверху мощностью множества внутренних состояний:

$$T_G < 2^{M_G} = 2^{M_{C_1}+M_{C_2}+M_R},$$

причем верхняя граница является заведомо недостижимой (достаточно рассмотреть цикл единичной длины, образованный состоянием генератора, в котором все ячейки памяти имеют нулевые значения).

Как было отмечено выше, за счет лавинного эффекта период последовательности внутренних состояний клеточных автоматов не может быть меньше величины периода T_R выходной последовательности регистра R. Известно [20], что максимальный период вы-

ходной последовательности двоичного регистра сдвига с линейными обратными связями составляет $2^{M_R} - 1$ и достигается в том и только том случае, если характеристический многочлен регистра является примитивным над полем $\mathbb{F}_2$. Таким образом, если регистр сдвига R вырабатывает последовательность максимального периода, то нижняя граница периода последовательности внутренних состояний генератора составляет

$$2^{M_R} - 1 \leqslant T_G.$$

Учитывая, что на каждом такте работы генератор вырабатывает 256 бит, для периода T его выходной последовательности справедливы следующие ограничения:

$$256 \cdot \left(2^{M_R} - 1\right) \leqslant T < 256 \cdot 2^{M_{C_1} + M_{C_2} + M_R}.$$

Отметим, что нижняя граница периода выходной последовательности целиком определяется длиной регистра сдвига с линейными обратными связями. В разработанных генераторах используется регистр длины 63; съем значений обратной связи осуществляется с первой и последней ячеек регистра (характеристический многочлен $f(x) = x^{63} + x + 1$ является примитивным над $\mathbb{F}_2$).

При построении генератора на основе классических клеточных автоматов $M_{C_1} = M_{C_2} = 37 \cdot 11 = 407$ и $M_G = 877$, что дает оценку длины периода выходной последовательности

$$2{,}36 \cdot 10^{21} \approx 256 \cdot \left(2^{63} - 1\right) \leqslant T < 2^{877} \approx 1{,}01 \cdot 10^{264}.$$

Аналогично для генератора на основе неоднородных клеточных автоматов $M_{C_1} = M_{C_2} = 257$, $M_G = 577$ и

$$2{,}36 \cdot 10^{21} \approx 256 \cdot \left(2^{63} - 1\right) \leqslant T < 2^{577} \approx 4{,}95 \cdot 10^{173}.$$

Гарантированная величина периода выходной последовательности $T \geqslant 2{,}36 \cdot 10^{21}$ бит является достаточной для подавляющего большинства практических применений; тем не менее, она может быть увеличена за счет использования регистров сдвига большей длины. При этом следует учитывать, что на практике период выходной последовательности генератора определяется наименьшим общим кратным периодов внутренних состояний

клеточных автоматов и значительно превосходит нижнюю оценку.

8. Исследование статистических свойств выходных последовательностей генераторов

Исследование выходных последовательностей разработанных генераторов было направлено на поиск параметров клеточных автоматов, обеспечивающих хорошие статистические свойства. В качестве инструмента исследования применялся набор статистических тестов [21], разработанный Национальным институтом стандартов и технологии (NIST) США. В состав набора входят 15 разновидностей тестов, каждая из которых направлена на выявление отклонений определенных характеристик от ожидаемых для случайной последовательности с равномерным распределением.

Оценка статистических свойств последовательностей требует значительного объема аппаратных ресурсов (в первую очередь, процессорного времени), поэтому тестирование было организовано по итеративной схеме и включало две фазы: предварительную и основную, различающиеся наборами тестов и длиной исследуемых последовательностей (табл. 1).

На предварительной фазе проводился сокращенный набор тестов для выходных последовательностей небольшой длины. Это позволило на ранней стадии исключить генераторы, выходные последовательности которых обладают существенными статистическими недостатками.

На основной фазе набор тестов выполнялся в полном объеме. Длина последовательностей и параметры тестов были выбраны в соответствии с рекомендациями NIST [21]. Тестирование включало в себя три итерации, причем на каждой последующей итерации исследовались генераторы, показавшие наилучшие результаты (т. е. успешно прошедших наибольшее количество тестов) на предыдущей. Последняя — третья — итерация основной фазы выполнялась до обнаружения генератора, успешно проходящего все тесты.

В результате проведенного исследования были обнаружены два набора параметров генератора на основе классических клеточных автоматов и один набор параметров генератора на основе неоднородных клеточных автоматов, при которых выходные после-

Таблица 1. Параметры предварительной и основной фаз статистического тестирования генераторов псевдослучайных последовательностей.

Параметр	Предварит. фаза	Основная фаза
Объект тестирования		
Количество генераторов каждого типа	10 000	100 / 10 / X[1]
Количество последовательностей для каждого генератора	1 000	10 / 100 / 1000[1]
Длина каждой последовательности, бит	1 024	1 024 000
Состав тестов		
Frequency (Monobit) Test	√	√
Frequency Test within a Block	√	√
Runs Test	√	√
Test for the Longest Run of Ones in a Block	√	√
Binary Matrix Rank Test		√
Discrete Fourier Transform (Spectral) Test		√
Non-overlapping Template Matching Test		√
Overlapping Template Matching Test		√
Maurer's Universal Statistical Test		√
Linear Complexity Test		√
Serial Test		√
Approximate Entropy Test		√
Cumulative Sums (Cusum) Test	√	√
Random Excursions Test		√
Random Excursions Variant Test		√
Параметры тестов		
Frequency Test within a Block: длина подпоследовательности M	20	10 240
Non-overlapping Template Matching Test: длина шаблона m	Н/Д	9
Overlapping Template Matching Test: длина шаблона m	Н/Д	9
Linear Complexity Test: размер блока M	Н/Д	1 000
Serial Test: длина шаблона m	Н/Д	16
Approximate Entropy Test: длина шаблона m	Н/Д	10

[1] Указаны значения для первой / второй / третьей итерации основной фазы

довательности указанных генераторов успешно проходят все тесты из набора NIST, т. е. соответствуют по своим свойствам случайным двоичным последовательностям с равномерным распределением.

9. Аппаратная реализация

Автором был разработан действующий макет аппаратной реализации предложенных генераторов. В качестве платформы для реализации используется недорогая ПЛИС (FPGA) семейства Altera Cyclone II. Выходная псевдослучайная последовательность генератора подается напрямую на выводы микросхемы ПЛИС, а также записывается во внутреннюю память для дальнейшего анализа (рис. 4).

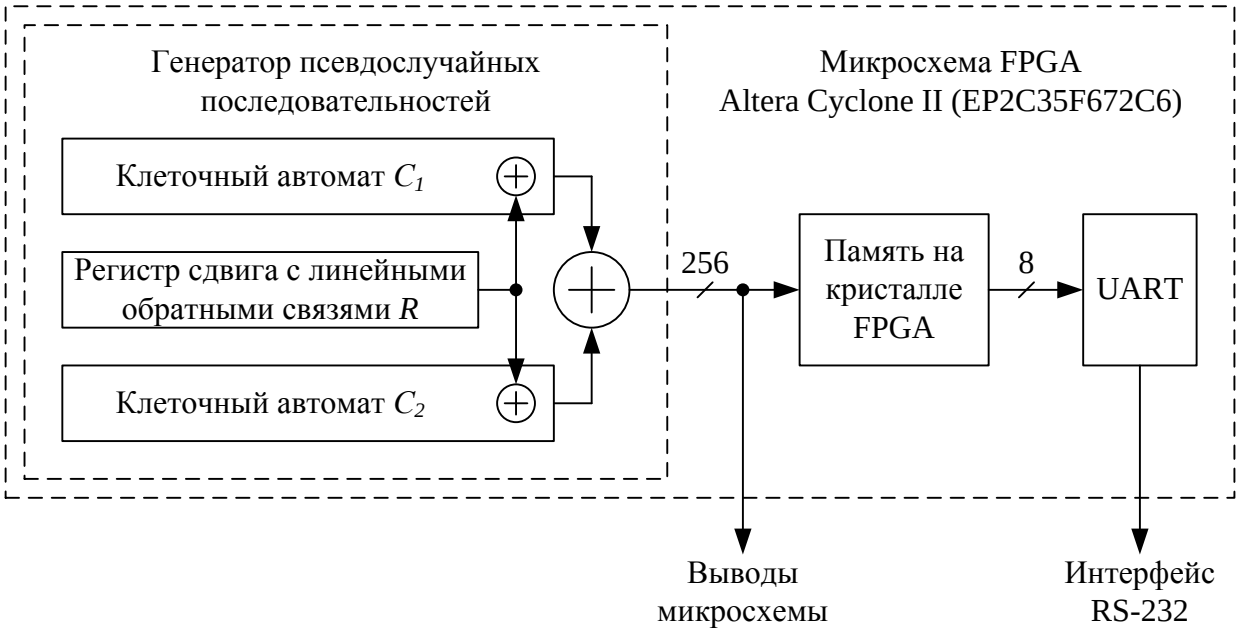

Рис. 4. Структурная схема макета аппаратной реализации генераторов псевдослучайных последовательностей на основе клеточных автоматов.

Номинальная частота схемы составляет 100 МГц, причем статический анализ временны́х задержек, проведенный в САПР Altera Quartus II, показал, что она может быть увеличена до 140 МГц при построении генератора на основе классических клеточных автоматов и до 149 МГц — при использовании неоднородных.

Параллельная структура клеточных автоматов позволяет обеспечить вычисление нового состояния и формирование 256 бит выхода за один такт синхронизации схемы. Таким образом, на номинальной тактовой частоте скорость выработки выходной последователь-

ности составляет 23,8 Гбит/с.

Для сравнения быстродействия аппаратной реализации были выбраны наиболее современные поточные шифры, представленные на европейский конкурс eSTREAM. Сравнение проводилось по двум показателям: скорости выработки выходной последовательности на максимальной тактовой частоте и на частоте 100 МГц. Использование различных показателей обусловлено тем, что авторы работы [22], на которой основываются наши данные о быстродействии шифров, рассматривали реализацию алгоритмов в рамках технологии заказных микросхем ASIC, позволяющей достичь в несколько раз более высоких частот по сравнению с FPGA (при этом технология ASIC является гораздо более затратной и экономически выгодна только при серийном производстве).

Как видно из рис. 5, разработанная реализация превосходит лучший из аналогов — алгоритм Trivium — по быстродействию на максимальной частоте в два, а на частоте 100 МГц — в четыре раза.

Помимо быстродействия важную роль играет эффективность реализации, которая выражается в скорости выработки выходной последовательности на единицу использованных аппаратных ресурсов (для FPGA Altera такой единицей является логический элемент — LE).

Результаты сравнения эффективности представлены на рис. 6 (данные об эффективности аппаратной реализации шифров получены из [23]). Наибольшую эффективность, существенно превосходящую аналоги, обеспечивает генератор на основе неоднородных клеточных автоматов, что объясняется малой мощностью окрестности. При этом эффективность реализации генератора на основе классических клеточных автоматов является довольно невысокой.

Заключение

В работе были представлены новые генераторы псевдослучайных последовательностей с равномерным распределением, основанные на использовании классических и неоднородных клеточных автоматов.

Выходные последовательности таких генераторов обладают хорошими статистиче-

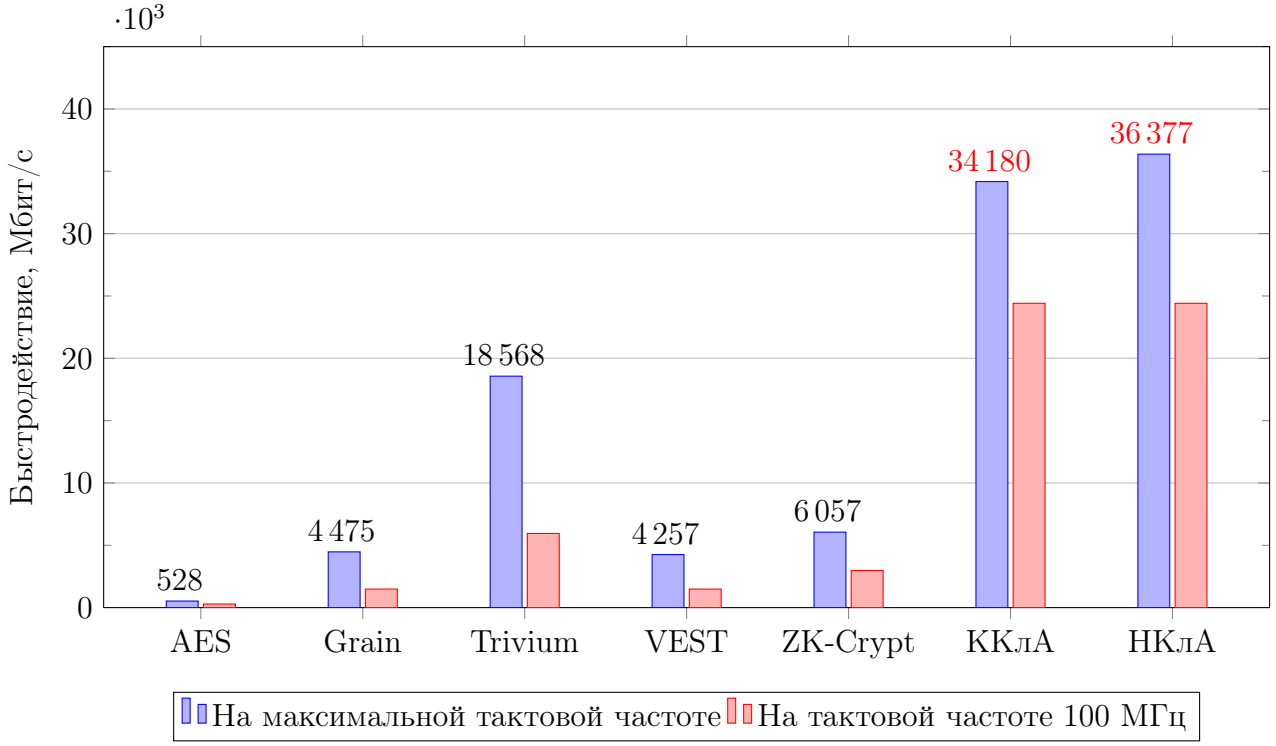

Рис. 5. Сравнение быстродействия разработанной аппаратной реализации и поточных шифров, представленных на европейский конкурс eSTREAM: ККлА — генератор на основе классических клеточных автоматов, НКлА — генератор на основе неоднородных клеточных автоматов.

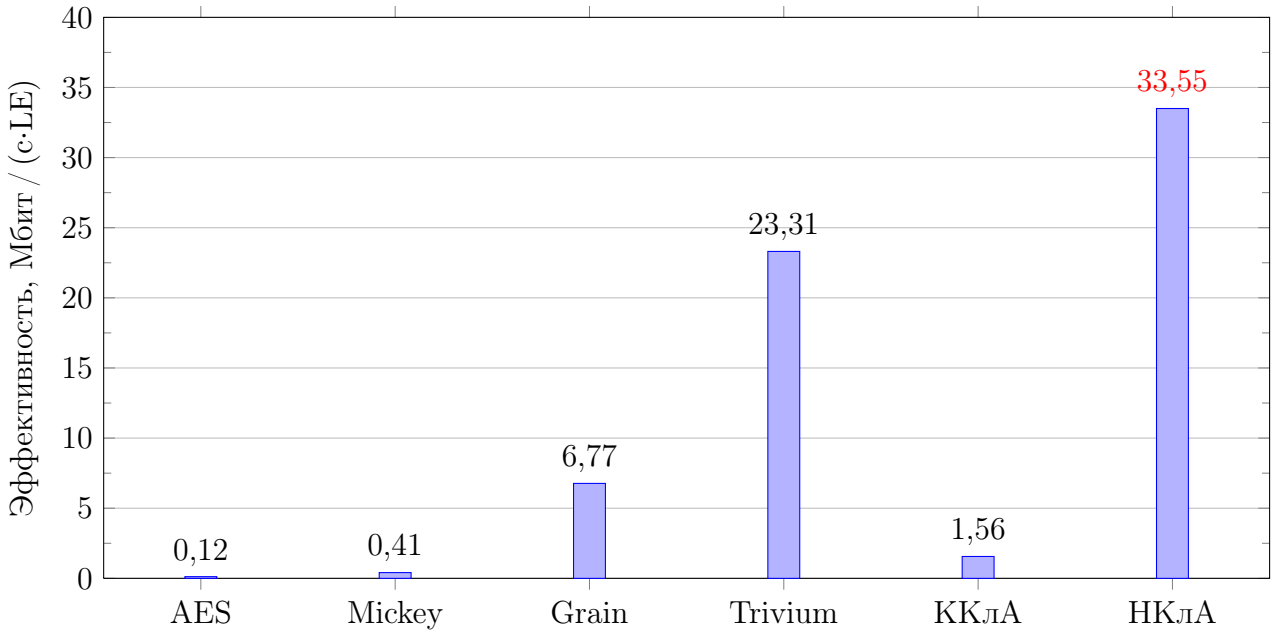

Рис. 6. Сравнение эффективности разработанной аппаратной реализации и поточных шифров, представленных на европейский конкурс eSTREAM: ККлА — генератор на основе классических клеточных автоматов, НКлА — генератор на основе неоднородных клеточных автоматов.

скими свойствами и успешно проходят наборы специализированных статистических тестов, а выбранная структура генераторов позволяет обеспечить любой наперед заданный период.

Разработанная автором аппаратная реализация генераторов на базе ПЛИС Altera Cyclone II обеспечивает быстродействие в 23,8 Гбит/с при тактовой частоте всего 100 МГц, что достигается за счет параллельного вычисления значений всех ячеек клеточных автоматов и формирования выхода генератора за один такт синхронизации схемы. Следует отметить, что высокое быстродействие может быть достигнуто при реализации на любых вычислительных устройствах с высокой степенью параллелизма, таких как графические процессоры (GPU), что позволяет говорить о возможности массового применения подобных алгоритмов.

Автор выражает благодарность Жукову Алексею Евгеньевичу за внимание к настоящей работе.

Список литературы

1. James F. A Review of Pseudorandom Number Generators // Computer Physics Communications, no. 60, 1990. Pp. 329 – 344.

2. Tippet L. Random Sampling Numbers. Cambridge University Press, 1927.

3. Kendall M., Babington-Smith B. Tables of Random Sampling Numbers. Cambridge University Press, 1939.

4. A Million Random Numbers with 100,000 Normal Deviates / The RAND Corporation. The Free Press, 1955. 625 p.

5. Marsaglia G. The Marsaglia Random Number CDROM Including the DIEHARD Battery of Tests of Randomness. URL: http://stat.fsu.edu/pub/diehard (дата обращения: 14.09.2010).

6. RANDOM.ORG — True Random Number Service. URL: http://www.random.org (дата обращения: 14.09.2010).

7. HotBits: Genuine Random Numbers, Generated by Radioactive Decay. URL: http://www.fourmilab.ch/hotbits (дата обращения: 14.09.2010).

8. Gentle E. Random Number Generation and Monte-Carlo Methods, 2nd. ed. Springer, 2005. 397 p.

9. Farmer D., Toffoli T. Preface to Cellular Automata // Proc. Interdisciplinary Workshop, 1984. Pp. vii – xii.

10. Тоффоли Т., Марголус Н. Машины клеточных автоматов: Пер. с англ. М.: Мир, 1991. 280 с.

11. Tomassini M., Perrenoud M. Stream Cyphers with One- and Two-Dimensional Cellular Automata // Lecture Notes in Computer Science, vol. 1917, 2000. Pp. 722 – 731.

12. Sipper M., Tomassini M. Computation in Artificially Evolved, Non-uniform Cellular Automata // Theor. Comput. Sci., vol. 217, no. 1, 1999. Pp. 81 – 98.

13. Non-Uniform Cellular Automata / Cattaneo G. [et al.] // Lecture Notes in Computer Science, vol. 5457, 2009. Pp. 302 – 313.

14. Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика, № 2, 2010. С. 34 – 41.

15. Харин Ю. С., Берник В. И., Матвеев Г. В. Математические основы криптологии: Уч. пос. Мн.: БГУ, 1999. 319 с.

16. Логачев О. А., Сальников А. А., Ященко В. В. Криптографические свойства дискретных функций. URL: http://www.ict.edu.ru/ft/002450/logachev_ea.pdf (дата обращения: 14.09.2010).

17. Wolfram S. Cellular Automata // Los Alamos Science, vol. 9, 1983. Pp. 2 – 21.

18. Wolfram S. Cryptography with Cellular Automata // Lecture Notes in Computer Science, vol. 218, 1986. Pp. 429 – 432.

19. Wolfram S. Random Sequence Generation by Cellular Automata // Advances in Applied Mathematics, vol. 7, 1986. Pp. 429 – 432.

20. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т.: Пер. с англ. М.: Мир, 1988. Т. 1. 430 с.

21. SP 800-22. A Satistical Test Suite for Random and Pseudorandom Number Generators for Cryprographic Applications, rev. 1a. / NIST, 2010. URL: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (дата обращения: 14.09.2010).

22. Hardware Evaluation of eSTREAM Candidates: Achterbahn, Grain, MICKEY, MOSQUITO, SFINKS, Trivium, VEST, ZK-Crypt / Gürkaynak F. K. [et al.], 2006. URL: http://www.ecrypt.eu.org/stream/papersdir/2006/015.pdf (дата обращения: 14.09.2010).

23. Rogawski M. Hardware Evaluation of eSTREAM Candidates: Grain, Lex, Mickey128, Salsa20 and Trivium. 2007. URL: http://www.ecrypt.eu.org/stream/papersdir/2007/025.pdf (дата обращения: 14.09.2010).