

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/8/5

УДК 004.421.5

ВЫСОКОСКОРОСТНЫЕ ГЕНЕРАТОРЫ
ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

Б. М. Сухинин

*Московский государственный технический университет им. Н. Э. Баумана, г. Москва,
Россия***E-mail:** b.sukhinin@gmail.com

Псевдослучайные последовательности (ПСП) широко используются в различных областях науки и техники — от моделирования физических процессов и методов Монте-Карло до криптографии. В работе исследуется ряд свойств однородных двумерных булевых клеточных автоматов, а также разрабатывается новый генератор псевдослучайных последовательностей, основанный на использовании этих автоматов. Выходные последовательности таких генераторов имеют хорошие статистические свойства, а аппаратная реализация предложенных алгоритмов на типовых ПЛИС обладает очень высоким быстродействием — до 25 Гбит/с на частоте 100 МГц.

Ключевые слова: генераторы псевдослучайных последовательностей, клеточные автоматы, лавинный эффект.

Введение

Клеточным автоматом (КЛА) называется модель с дискретным временем, состоящая из множества ячеек памяти, упорядоченных в периодическую n -мерную решетку [1]. Заполнения ячеек являются элементами некоторого конечного множества. Для каждой ячейки выбирается ее окрестность, которая используется для определения заполнения ячейки на следующем такте работы по некоторому заранее заданному правилу.

Для классических клеточных автоматов выполняются два свойства: однородности и локальности [2]. Однородность означает, что все ячейки КЛА являются неразличимыми по своим свойствам; кроме того, для решения проблемы краевых клеток противоположные края решетки отождествляются, то есть двумерная решетка закручивается в тор. В соответствии со свойством локальности в окрестность каждой ячейки входят только ячейки, удаленные от нее на расстояние не более заданного.

Обширные исследования одномерных клеточных автоматов были проведены Стефаном Вольфрамом (см., например, [3–5]); исследование же КЛА размерности 3 и более обладает ограниченным практическим интересом в силу сложности их реализации. Поэтому в настоящей работе рассматриваются двумерные булевы клеточные автоматы с прямоугольными ячейками. В таких автоматах заполнения ячеек памяти содержат двоичные значения; использование двоичного множества $\{0, 1\}$ и прямоугольная форма ячеек облегчают реализацию КЛА и их применение в вычислительной технике. В качестве правила, определяющего новые заполнения ячеек на следующем

такте работы, используется булева функция, аргументами которой являются заполнения ячеек, входящих в окрестность данной; такую функцию будем называть локальной функцией связи. В качестве окрестности ячейки используем подмножество ячеек, непосредственно смежных с данной, а также, возможно, ее саму; использование более широкого множества увеличивает число аргументов локальной функции связи и делает ее реализацию непрактичной.

1. Свойства клеточных автоматов

1.1. Зависимость числа единичных заполнений ячеек от веса локальной функции связи

Локальная функция связи является основным параметром, определяющим особенности функционирования клеточного автомата. Важной задачей является изучение зависимости между характеристиками локальной функции связи и распределением заполнений ячеек решетки клеточного автомата.

Рассмотрим локальную функцию связи f , вектор значений которой имеет длину 2^s , где s — число аргументов функции (оно совпадает с мощностью окрестности ячейки). Пусть вес функции f , то есть число наборов аргументов, на которых функция принимает единичные значения, равен ω . Относительным весом функции назовем величину $\omega_0 = \omega/2^s$.

Предположим, что начальные заполнения ячеек решетки распределены случайно и равновероятно, то есть для произвольной ячейки m

$$\Pr[m = 0] = \Pr[m = 1] = \frac{1}{2}.$$

В таком случае все возможные двоичные наборы $\Psi(m)$ длины s , соответствующие заполнениям ячеек из окрестности m , также будут встречаться с равной вероятностью.

Поскольку вес функции f равен ω и все наборы аргументов равновероятны, вероятности того, что функция f принимает единичное или нулевое значение на наборе $\Psi(m)$, составляют

$$\begin{aligned}\Pr[f(\Psi(m)) = 1] &= \omega/2^s = \omega_0, \\ \Pr[f(\Psi(m)) = 0] &= 1 - \omega_0.\end{aligned}$$

Напомним, что заполнение ячейки m на следующем такте работы клеточного автомата совпадает со значением локальной функции связи на наборе $\Psi(m)$. Из этого очевидным образом следует, что одинаковое количество единичных и нулевых заполнений ячеек достигается только при $\omega_0 = 1/2$, что соответствует равновесным локальным функциям связи.

На рис. 1 изображены графики временной зависимости отношения числа единичных заполнений к общему количеству ячеек КЛА при различных весах локальной функции связи. Данные отражают усреднение для 1 000 различных клеточных автоматов с размерами решетки 37×11 ячеек и случайно выбранной локальной функцией связи от 9 аргументов (длина вектора значений 512). На графиках хорошо видно, что каждому значению относительного веса ω_0 соответствует быстрое приближение к некоторому стационарному значению числа единичных ячеек клеточного автомата.

1.2. Характеристики лавинного эффекта

Понятие лавинного эффекта было введено Хорстом Фейстелем [6] в 1973 г. для оценки свойств криптографических преобразований. Лавинный эффект показывает,

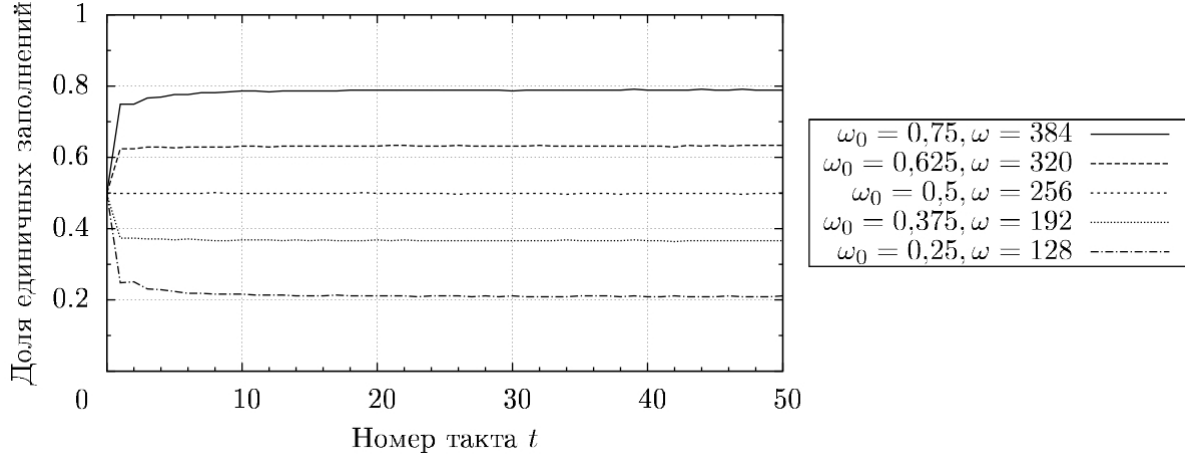


Рис. 1. Отношение числа единичных заполнений к общему количеству ячеек при различных весах локальной функции связи

насколько сильно изменяется выход некоторого преобразования при изменении одного бита входных данных.

Перед тем как перейти к описанию лавинного эффекта в двумерных клеточных автоматах, необходимо ввести несколько дополнительных понятий. Для этого рассмотрим клеточный автомат с решеткой размера $M_X \times M_Y$. Через $m_{(x,y)}$ обозначим ячейку с координатами (x, y) . Поскольку решетка КлА представляет собой тор, вычисления координат осуществляются по модулю соответствующего размера решетки, то есть

$$m_{(x,y)} \equiv m_{((x \bmod M_X), (y \bmod M_Y))}.$$

В дальнейшем для упрощения записи операцию взятия остатка от деления будем опускать.

Введем понятие расстояния между ячейками клеточного автомата как максимальное абсолютное значение разности соответствующих координат. С учетом закручивания решетки КлА в тор расстояние $\Delta(m_{(x_1,y_1)}, m_{(x_2,y_2)})$ между ячейками $m_{(x_1,y_1)}$ и $m_{(x_2,y_2)}$ задается формулой

$$\Delta(m_{(x_1,y_1)}, m_{(x_2,y_2)}) = \max(\min(|x_1 - x_2|, M_X - |x_1 - x_2|), \min(|y_1 - y_2|, M_Y - |y_1 - y_2|)).$$

Очевидно, что максимально возможное расстояние между двумя ячейками КлА равно

$$\Delta_{\max} = \max\left(\left\lfloor \frac{M_X - 1}{2} \right\rfloor, \left\lfloor \frac{M_Y - 1}{2} \right\rfloor\right).$$

Рассмотрим два идентичных клеточных автомата, т.е. автоматы с одинаковыми размерами решетки $M_X \times M_Y$ (для определенности будем считать, что $M_X \geq M_Y$), одной и той же локальной функцией связи и одинаковыми заполнениями совпадающих по координатам ячеек. Обозначим через $m_{(x,y)}^t$ заполнение ячейки первого клеточного автомата с координатами (x, y) в момент времени t ; для аналогичной ячейки второго клеточного автомата будем использовать обозначение $\hat{m}_{(x,y)}^t$. В момент времени $t = 0$ изменим заполнение ячейки с координатами $(0, 0)$ второго клеточного автомата на противоположное:

$$\hat{m}_{(0,0)}^0 \leftarrow 1 - \hat{m}_{(0,0)}^0$$

(поскольку в силу однородности все ячейки неразличимы по своим свойствам, выбор конкретной ячейки не ограничивает общности).

Лавинный эффект отражает распространение изменений, вызванных во втором клеточном автомате сменой заполнения одной ячейки памяти. Введём две числовые характеристики лавинного эффекта: интегральную и пространственную. Если изменения распространяются равномерно во всех направлениях с максимально возможной линейной скоростью (в данном случае составляющей одну ячейку за такт работы) и при этом изменяется заполнение половины всех ячеек, то такой лавинный эффект называется оптимальным.

Интегральной характеристикой лавинного эффекта $\eta(t)$ в клеточных автоматах назовем временную зависимость отношения числа несовпадающих заполнений для ячеек с одинаковыми координатами к общему количеству ячеек в решетке:

$$\eta(t) = \sum_{\substack{0 \leq x < M_X \\ 0 \leq y < M_Y}} \frac{m_{(x,y)}^t \oplus \hat{m}_{(x,y)}^t}{M_X \cdot M_Y},$$

где сумма вычисляется как обычное арифметическое сложение, а операция $\oplus$ — как сложение по модулю 2. Интегральная характеристика оптимального лавинного эффекта имеет вид

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

Показателем, отражающим линейную скорость распространения изменений по решетке клеточного автомата, является пространственная характеристика лавинного эффекта $\mu(t)$, равная отношению максимального расстояния, на котором проявились изменения, к максимально возможному расстоянию:

$$\mu(t) = \frac{1}{\lfloor (M_X - 1)/2 \rfloor} \cdot \max_{\substack{0 \leq x < M_X \\ 0 \leq y < M_Y}} ((m_{(x,y)}^t \oplus \hat{m}_{(x,y)}^t) \cdot \Delta(m_{(0,0)}, m_{(x,y)})),$$

где $\Delta(m_{(0,0)}, m_{(x,y)})$ — расстояние между ячейками с координатами $(0,0)$ и (x,y) . Пространственная характеристика оптимального лавинного эффекта описывается формулой

$$\mu_{\text{opt}}(t) = \begin{cases} \frac{t}{\lfloor (M_X - 1)/2 \rfloor}, & t < \lfloor (M_X - 1)/2 \rfloor; \\ 1, & t \geq \lfloor (M_X - 1)/2 \rfloor. \end{cases}$$

Следует отметить, что лавинный эффект в конкретном клеточном автомате зависит от выбора начального заполнения ячеек решетки и локальной функции связи.

Таким образом, характеристики лавинного эффекта отражают свойства автомата в целом и должны рассматриваться как некоторый усредненный показатель. Кроме того, лавинный эффект существенно зависит от выбора окрестности, то есть от числа аргументов локальной функции связи. Из графиков характеристик лавинного эффекта, приведенных на рис. 2 и 3, видно, что характеристики приближаются к оптимальным по мере увеличения числа аргументов локальной функции связи; кроме того, графики для 8 и 9 аргументов являются практически идентичными, поэтому будем использовать локальные функции связи от 8 аргументов. Данные получены усреднением по 1 000 различным клеточным автоматам с размерами решетки 37×11 ячеек.

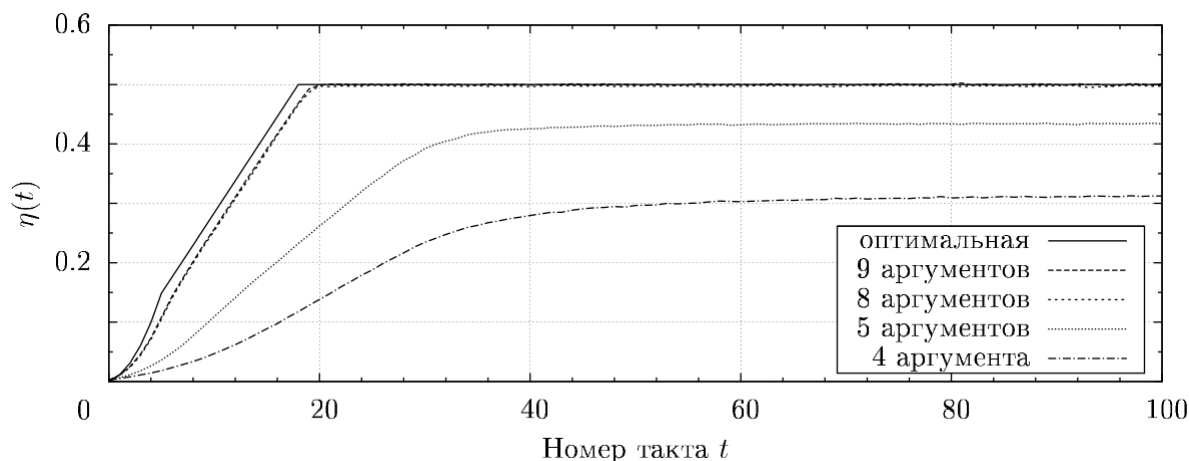


Рис. 2. Интегральная характеристика лавинного эффекта

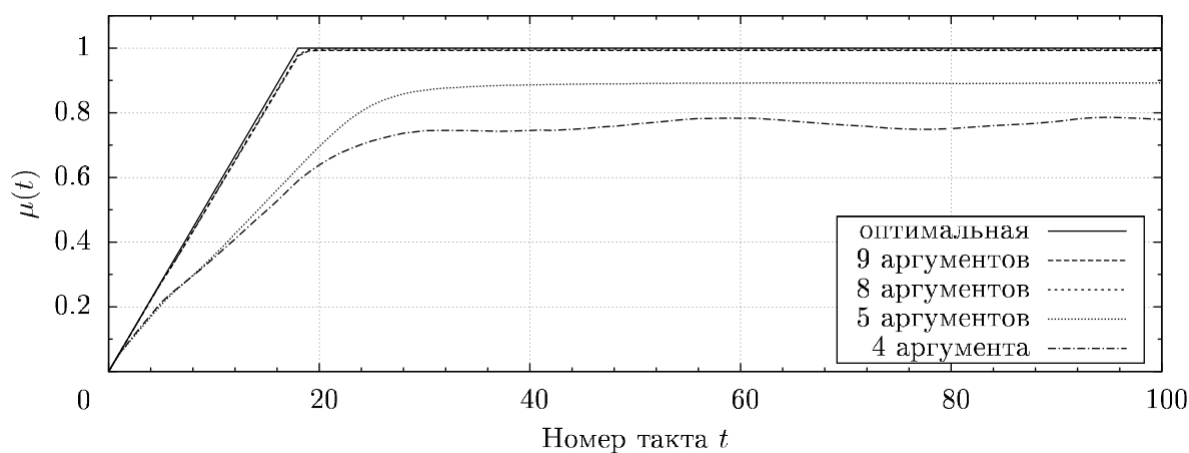


Рис. 3. Пространственная характеристика лавинного эффекта

1.3. Периодичность клеточных автоматов

Клеточные автоматы можно рассматривать как автономные конечные автоматы. Как и любой автономный конечный автомат, КЛА обладают конечным периодом последовательности внутренних состояний, то есть заполнений ячеек решетки. В силу нелинейности локальной функции связи оценить период клеточного автомата не представляется возможным; тем не менее можно дать рекомендации по его увеличению.

Помимо классических временных периодов клеточных автоматов рассматриваем пространственные периоды, характеризующиеся следующим соотношением:

$$m_{(x,y)} = m_{((x+T_X),(y+T_Y))},$$

где $T_X \leq M_X$ и $T_Y \leq M_Y$ — величины пространственных периодов по горизонтали и вертикали соответственно. Очевидно, что для существования периода необходимо, чтобы его величина вдоль некоторой оси делила размер решетки вдоль той же оси. Для описания клеточных автоматов с установившимся пространственным периодом достаточно рассматривать подрешетку размера $T_X \times T_Y$; следствием этого является существенное снижение периода КЛА.

На свойства периодичности также влияет структура связей клеточного автомата. На рис. 4 приведены графики пространственной характеристики лавинного эффекта, полученные в течение 300 тактов работы автомата. Колебания графика, соответствующего локальной функции связи с 4 аргументами, вызваны установившимся временным периодом. Кроме того, из рисунка видно, что с увеличением числа аргументов вероятность возникновения таких периодов резко сокращается.

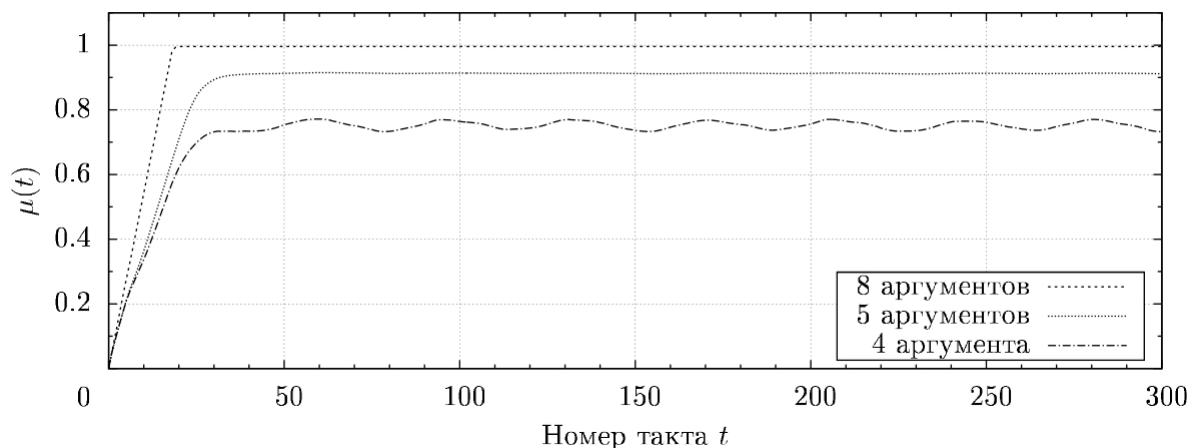


Рис. 4. Проявление периодичности на графике пространственной характеристики лавинного эффекта

2. Генераторы ПСП на основе клеточных автоматов

2.1. Структура генератора

Структура генератора ПСП, основанного на использовании однородных двумерных булевых клеточных автоматов, приведена на рис. 5. В состав генератора входят два клеточных автомата и регистр сдвига с линейной обратной связью (РСЛОС).

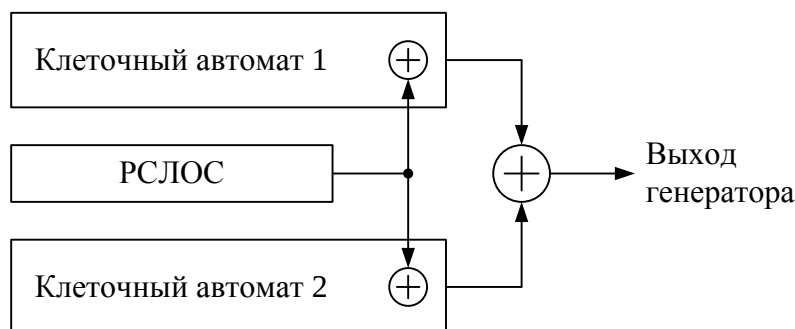


Рис. 5. Структура генератора ПСП на основе клеточных автоматов

Размеры решетки одинаковы для обоих автоматов и составляют 37×11 ячеек; выбор простых чисел позволяет избежать возникновения пространственных периодов. Окрестность каждой ячейки состоит из ячеек, непосредственно смежных с ней, что соответствует локальной функции связи от 8 аргументов. В качестве выхода клеточного автомата используются заполнения ячеек подрешетки размера 32×8 , то есть ячеек $m_{(x,y)}$, где $0 \leq x < 32$ и $0 \leq y < 8$, что обеспечивает выработку каждым КЛА 256 бит за один такт работы. Для каждого клеточного автомата используется своя собственная равновесная локальная функция связи.

Выход РСЛОС на каждом такте работы прибавляется по модулю 2 к заполнениям ячеек клеточных автоматов с координатами (34, 9). Лавинный эффект позволяет гарантировать, что период внутренних состояний клеточных автоматов будет не меньше периода выходной последовательности РСЛОС. Считаем, что для практического применения генератора достаточно использовать РСЛОС длины 63, что обеспечивает период его выходной последовательности $2^{63} - 1 \approx 9,2 \cdot 10^{18}$ бит; период выходной последовательности КЛА при этом составляет не менее $32 \cdot 8 \cdot (2^{63} - 1) \approx 2,4 \cdot 10^{21}$ бит. Тем не менее длина регистра может быть изменена при необходимости.

Выход генератора формируется посредством сложения по модулю 2 выходных последовательностей обоих клеточных автоматов, что позволяет существенно улучшить статистические свойства выходной последовательности генератора, увеличить ее период, а также затруднить восстановление внутреннего состояния генератора по выходным значениям.

2.2. Аппаратная реализация и статистические свойства генератора

Автором был разработан прототип аппаратной реализации предложенного генератора на ПЛИС Altera Cyclone II (EP2C35F672C6); структурная схема прототипа приведена на рис. 6. Выходная последовательность генератора подавалась напрямую на выходы микросхемы ПЛИС, а также записывалась для дальнейшего анализа во внутреннюю память. Параллельная структура клеточных автоматов позволила достичь вычисления нового состояния обоих КЛА и формирования выхода генератора за один такт синхронизации схемы.

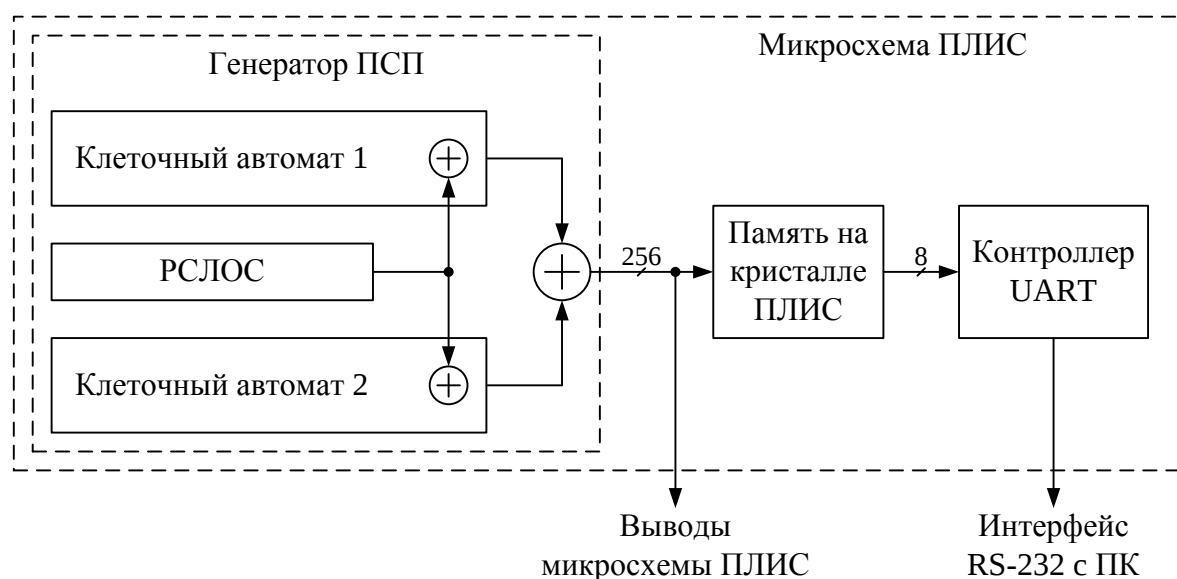


Рис. 6. Структурная схема прототипа аппаратной реализации генератора ПСП на ПЛИС

Рабочая частота схемы составила 100 МГц, причем статический анализ временных задержек показал, что она может быть повышена до 130 МГц без внесения каких-либо изменений. Учитывая, что на каждом такте работы генератор формирует 256 бит выходной последовательности, скорость ее выработки составила 23,8 Гбит/с.

Для исследования статистических свойств выходной последовательности использовался набор тестов NIST [7], включающий в себя 15 разновидностей проверок, направленных на выявление различных статистических отклонений исследуемой последовательности от истинно случайной. Следует отметить, что набор NIST предназначен для

тестирования криптографических генераторов псевдослучайных последовательностей, то есть в нем предъявляются наиболее жесткие требования. Тестирование генераторов с различными локальными функциями связи клеточных автоматов позволило обнаружить функции, при которых генератор успешно проходит все тесты из набора. Для сокращенной версии генератора, в которой один из двух клеточных автоматов отключен и не вырабатывает выходную последовательность, таких функций обнаружено не было. Тем не менее следует учитывать, что сокращенный генератор может использоваться в областях, где предъявляются менее жесткие требования к статистическим свойствам ПСП.

Заключение

В работе исследованы некоторые свойства однородных двумерных булевых клеточных автоматов и предложена структура генератора псевдослучайных последовательностей, основанного на использовании КлА. Выходные последовательности такого генератора успешно проходят набор статистических тестов NIST, предъявляющий наиболее жесткие требования к генераторам ПСП. Разработанный прототип аппаратной реализации генератора обеспечивает выработку выходной последовательности на сверхвысокой скорости до 25 Гбит/с.

Необходимо отметить, что использование клеточных автоматов предоставляет большое поле для исследований. В настоящее время ведется работа над программной реализацией генератора, использующей в качестве вычислительного устройства графический адаптер ПЭВМ, что позволит говорить о возможности массового применения подобных алгоритмов. Кроме того, одним из объектов исследований являются неоднородные клеточные автоматы, в которых окрестность каждой ячейки выбирается случайным образом, но при этом является фиксированной в течение работы КлА. Такие клеточные автоматы обладают существенно лучшими характеристиками по сравнению с рассмотренными выше, а также позволяют строить намного более эффективные реализации.

ЛИТЕРАТУРА

1. *Farmer D., Toffoli T., Wolfram S.* Preface to Cellular Automata // Proceedings of an Interdisciplinary Workshop. Los Alamos, New Mexico, 1984. P. vii–xii.
2. *Толффоли Т., Марголюс Н.* Машины клеточных автоматов. М.: Мир, 1991. 280 с.
3. *Wolfram S.* A New Kind of Science. Wolfram Media, 2002. 1192 p.
4. *Wolfram S.* Cellular Automata // Los Alamos Science. 1983. No. 9. P. 2–21.
5. *Wolfram S.* Cryptography with Cellular Automata // Proceedings of CRYPTO'85. 1986. P. 429–432.
6. *Feistel H.* Cryptography and Computer Privacy // Scientific American. 1973. V. 228. No. 5. P. 15–23.
7. <http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf> — NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, revision 1.