УДК 004.421.5

Б. М. Сухинин

О НЕКОТОРЫХ СВОЙСТВАХ КЛЕТОЧНЫХ АВТОМАТОВ И ИХ ПРИМЕНЕНИИ В СТРУКТУРЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Исследованы свойства однородных двумерных булевых клеточных автоматов, а также разработан 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.

E-mail: b.sukhinin@gmail.com

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

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 КлА выполняются 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, т.е. 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 КлА были проведены Стефаном Вольфрамом [3–5]; исследования же КлА размерности 3 и более ограниченны в силу сложности их реализации. В настоящей работе будем рассматривать двумерные булевы КлА 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 используется подмножество ячеек, смежных с данной, а также, возможно, она сама. Использование более широкого множества увеличивает число аргументов локальной функции связи и делает ее реализацию непрактичной.

Свойства клеточных автоматов. *Зависимость числа единичных заполнений ячеек от веса локальной функции связи.* Локальная функция связи является основным параметром, определяющим особенности функционирования КлА. Важной задачей является изучение связи между характеристиками локальной функции связи и распределением заполнений ячеек решетки КлА.

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, т.е. число наборов аргументов, на которых функция принимает единичные значения, равно ω. Относительным весом функции назовем величину $\omega_0 = \omega/2^s$.

Предположим, что начальные заполнения ячеек решетки распределены случайно и равновероятно, т.е. для произвольной ячейки m имеем

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

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 соответственно

$$\Pr[f(\Psi(m)) = 1] = \omega/2^s = \omega_0,$$

$$\Pr[f(\Psi(m)) = 0] = 1 - \omega_0.$$

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

На рис. 1 изображены графики временно́й зависимости отношения числа единичных заполнений к общему числу ячеек КлА для различных весов локальной функции связи. Данные отражают усреднение для 1 000 различных КлА 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 КлА.

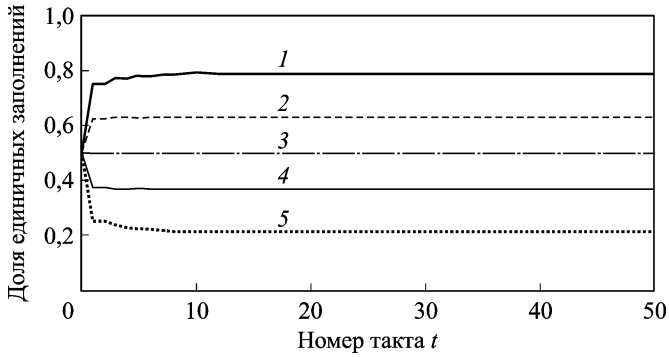

Рис. 1. Отношение числа единичных заполнений к общему числу ячеек при различных весах локальной функции связи:
1 — $\omega_0 = 0{,}75$; *2* — $\omega_0 = 0{,}625$; *3* — $\omega_0 = 0{,}5$; *4* — $\omega_0 = 0{,}375$; *5* — $\omega_0 = 0{,}25$

Характеристики лавинного эффекта. Понятие лавинного эффекта было введено Хорстом Фейстелем [6] в 1973 г. для оценки свойств криптографических преобразований. Лавинный эффект показывает, насколько сильно изменяется выход некоторого преобразования при изменении одного бита входных данных.

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

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

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

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

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

Очевидно, что максимально возможное расстояние между двумя ячейками КлА равно

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

Рассмотрим два идентичных КлА, т. е. 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 $m^t_{(x,y)}$ заполнение ячейки первого КлА с координатами (x, y) в момент времени t; для аналогичной ячейки второго КлА будем использовать обозначение $\hat{m}^t_{(x,y)}$. В момент времени $t = 0$ изменим заполнение ячейки с координатами $(0, 0)$ второго КлА на противоположное:

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

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

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

Интегральной характеристикой лавинного эффекта $\eta(t)$ в КлА назовем временну́ю зависимость отношения числа несовпадающих заполнений для ячеек с одинаковыми координатами к общему числу ячеек в решетке:

$$\eta(t) = \sum_{\substack{0 \le x < M_X \\ 0 \le y < M_Y}} \frac{m^t_{(x,y)} \oplus \hat{m}^t_{(x,y)}}{M_X M_Y},$$

где сумма $\sum$ вычисляется обычным арифметическим сложением, а операция $\oplus$ — сложение по модулю 2. Интегральная характеристика оптимального лавинного эффекта имеет вид

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

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

$$\mu(t) = \frac{1}{\lceil (M_X - 1)/2 \rceil} \max_{\substack{0 \le x < M_X \\ 0 \le y < M_Y}} \left((m^t_{(x,y)} \oplus \hat{m}^t_{(x,y)}) \cdot \Delta(m_{(0,0)}, m_{(x,y)}) \right),$$

где $\Delta(m_{(0,0)}, m_{(x,y)})$ — расстояние между ячейками с координатами $(0, 0)$ и (x, y), $\oplus$ — сложение по модулю 2. Пространственная характе-

ристика оптимального лавинного эффекта описывается формулой

$$\mu_{\text{opt}}(t) = \begin{cases} \dfrac{t}{\lceil (M_X - 1)/2 \rceil}, & t < \lceil (M_X - 1)/2 \rceil, \\ 1, & t \geq \lceil (M_X - 1)/2 \rceil. \end{cases}$$

Следует отметить, что лавинный эффект в конкретном КлА зависит от выбора начального заполнения ячеек решетки и локальной функции связи. Таким образом, характеристики лавинного эффекта отражают свойства КлА в целом и должны рассматриваться как некоторый усредненный показатель. Кроме того, лавинный эффект существенно зависит от выбора окрестности, т.е. от числа аргументов локальной функции связи. Из графиков характеристик лавинного эффекта, приведенных на рис. 2 и 3, следует, что характеристики приближаются к оптимальным по мере увеличения числа аргументов локальной функции связи; кроме того, графики для 8 и 9 аргументов являются

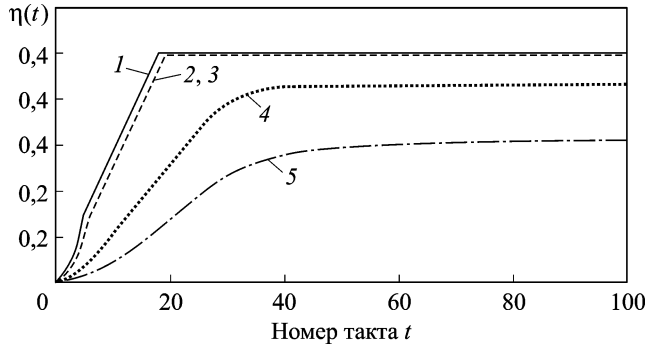

Рис. 2. Интегральная характеристика лавинного эффекта:
1 — оптимальная; *2* — 9 аргументов; *3* — 8 аргументов; *4* — 5 аргументов; *5* — 4 аргумента

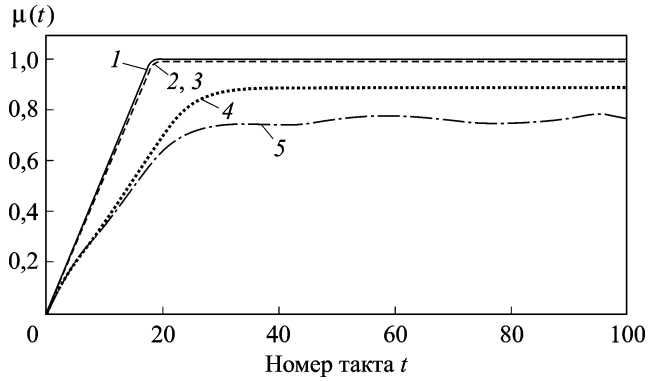

Рис. 3. Пространственная характеристика лавинного эффекта (*1*... *5* — см. рис. 2)

практически идентичными, поэтому мы будем использовать локальные функции связи от 8 аргументов. Данные получены усреднением по 1 000 различным КлА с размерами решетки 37×11 ячеек.

Периодичность КлА. Клеточные автоматы можно рассматривать как автономные конечные автоматы. Как и любые автономные конечные автоматы КлА имеют конечный период последовательности внутренних состояний, т.е. заполнений ячеек решетки. В силу нелинейности локальной функции связи оценить период КлА не представляется возможным; тем не менее можно дать рекомендации по его увеличению.

Помимо классических временны́х периодов КлА рассмотрим пространственные периоды, характеризующиеся следующим соотношением:

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

где $T_X \le M_X$ и $T_Y \le M_Y$ — пространственные периоды по горизонтали и вертикали соответственно. Очевидно, что для существования периода необходимо, чтобы его значение вдоль некоторой оси делило размер решетки вдоль той же оси. Для описания КлА 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 КлА. На рис. 4 приведены графики пространственной характеристики лавинного эффекта, полчученные в течение 300 тактов работы КлА. Колебания графика, соответствующего локальной функции связи с 4 аргументами, вызваны установившимся временным периодом. Из рис. 4 также следует, что с увеличением числа аргументов вероятность возникновения таких периодов резко сокращается.

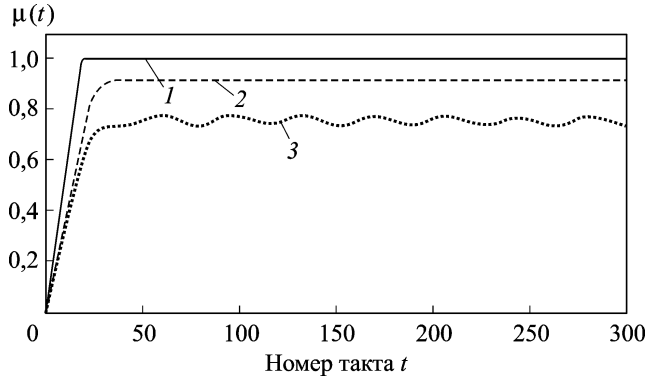

Рис. 4. Проявление периодичности на графике пространственной характеристики лавинного эффекта:
1 — 8 аргументов; *2* — 5 аргументов; *3* — 4 аргумента

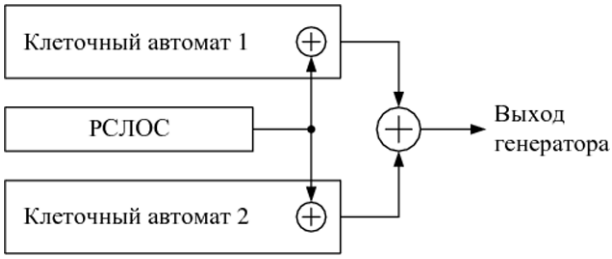

Рис. 5. Структура генератора ПСП на основе КлА

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

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 КлА используются заполнения ячеек подрешетки размера 32×8, т.е. ячеек $m_{(x,y)}$, где $0 \le x < 32$ и $0 \le y < 8$, что обеспечивает выработку каждым КлА 256 бит за один такт работы. Для каждого КлА используется своя собственная равновесная локальная функция связи.

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

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

Аппаратная реализация и статистические свойства генератора. Автором настоящей работы был разработан прототип аппаратной реализации предложенного генератора на ПЛИС Altera Cyclone II (EP2C35F672C6), структурная схема которого приведена на рис. 6. Выходная последовательность генератора подавалась напрямую на выводы ПЛИС, а также записывалась для дальнейшего анализа во внутрен-

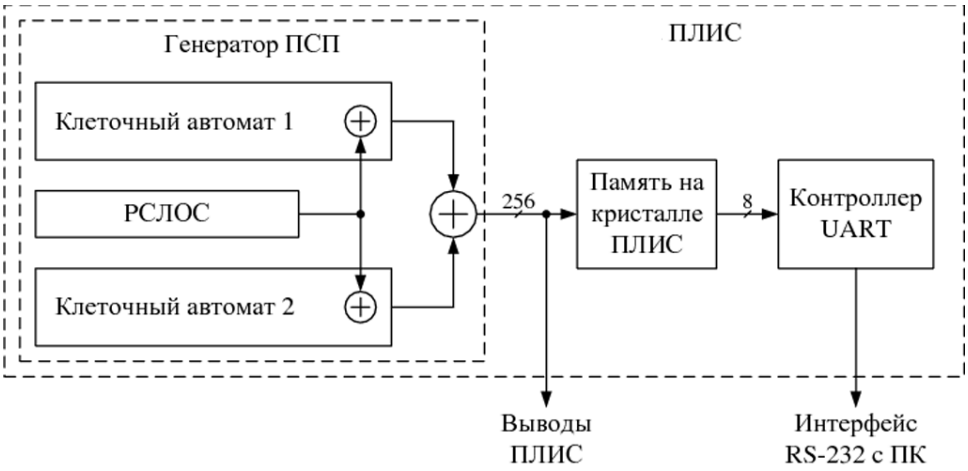

Рис. 6. Структурная схема прототипа аппаратной реализации генератора ПСП на ПЛИС

нюю память. Параллельная структура КлА позволила достичь вычисления нового состояния обоих КлА и формирования выхода генератора за один такт синхронизации схемы.

Рабочая частота схемы составила 100 МГц, причем статический анализ временных задержек показал, что частота 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 ПСП, т.е. в нем предъявляются наиболее жесткие требования. Тестирование генераторов с различными локальными функциями связи КлА позволило обнаружить функции, при которых генератор успешно проходит все тесты из набора. Для сокращенной версии генератора, в которой один из двух КлА 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 были исследованы некоторые свойства однородных двумерных булевых КлА 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.

Следует отметить, что использование КлА 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 КлА, в которых окрестность каждой ячейки выбирается случайным образом, но при этом является фиксированной в течение работы КлА; такие КлА имеют существенно лучшие характеристики по сравнению с рассмотренными в настоящей работе, а также позволяют строить намного более эффективные реализации.

СПИСОК ЛИТЕРАТУРЫ

1. F a r m e r D., T o f f o l i T., W o l f r a m S. Preface to cellular automata // Proceedings of an Interdisciplinary Workshop, 1984. – C. VII–XII.
2. Т о ф ф о л и Т., М а р г о л у с Н. Машины клеточных автоматов. – М.: Мир, 1991. – 280 с.
3. W o l f r a m S. A new kind of science. – Wolfram Media, 2002. – 1192 p.
4. W o l f r a m S. Cellular automata // Los Alamos Science, 1983. – No. 9. – P. 2–21.
5. W o l f r a m S. Cryptography with cellular automata // Proc. of CRYPTO'85, 1986. – P. 429–432.
6. F e i s t e l H. Cryptography and computer privacy // Scientific American, 1973. – Vol. 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.

Статья поступила в редакцию 16.04.2010

Борис Михайлович Сухинин родился в 1984 г., окончил в 2007 г. МГТУ им. Н.Э. Баумана. Ассистент кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор более 10 научных работ в области теории клеточных автоматов и генераторов псевдослучайных последовательностей.

B.M. Sukhinin (b. 1984) graduated from the Bauman Moscow State Technical University in 2007. Assistant lecturer of "Information Security" department of the Bauman Moscow State Technical University. Author of more than 10 publications in the field of cellular automata and generators of pseudorandom sequences.