УДК 004.056.55

В. В. ЖИХАРЕВИЧ, С. Э. ОСТАПОВ

Черновицкий национальный университет им. Ю. Федьковича, Украина

ИССЛЕДОВАНИЕ ОБРАТИМОСТИ ПРОГРАММНЫХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

В статье проанализирована проблема обратимости классических клеточных автоматов, используемых в качестве генераторов псевдослучайных бинарных последовательностей. Предложена модификация, базирующаяся на псевдослучайном механизме определения локализации взаимодействующих клеток и обеспечивающая необратимость. Исследована проблема самоорганизации динамики генератора. Причиной такого поведения является спонтанное уменьшение количества взаимодействующих клеток массива. Предложен подход, предотвращающий самоорганизацию модифицированных генераторов и базирующийся на обеспечении взаимодействия всех клеток массива.

Ключевые слова: *криптография, клеточные автоматы, обратимость.*

Введение

Идею использования классических клеточных автоматов (КА) для генерирования псевдослучайных бинарных последовательностей для криптографических применений впервые было высказано Стивеном Вольфрамом [1] в 80-х годах прошлого века. Он также предложил использование для этого определённых правил взаимодействий, в частности так называемого «правила 30». С тех пор достаточно большое количество исследователей пытались реализовать эти предложения и достигли определённых успехов [2-4]. Существуют также попытки построения блочной симметричной криптосистемы с применением КА [5, 6]. Однако, в перечисленных работах не проводятся оценки криптографической стойкости разработанных систем, их зависимости от входных условий и ряд других характеристик. В частности, не проводится анализ обратимости генерируемых последовательностей, что является существенным фактором для криптографической стойкости систем защищённой передачи информации.

Цель статьи – провести исследование обратимости программных генераторов псевдослучайных бинарных последовательностей на основе клеточных автоматов и сформулировать рекомендации относительно таких модификаций существующих алгоритмов, чтоб генерируемые ими последовательности были необратимыми.

1. Анализ обратимости классических КА

В работе [1] С. Вольфрам предложил использовать в качестве генератора псевдослучайных чисел одномерный клеточный автомат (КА), представляющий собой массив клеток c_1, c_2, …, c_n, состояния которых в следующий момент времени определяется по правилу:

$$c_i' = c_{i-1} \oplus (c_i \vee c_{i+1}). \quad (1)$$

Данное правило иногда называют «правилом 30». Псевдослучайная последовательность битов может генерироваться любой из n клеток одномерного массива.

Несмотря на достаточно хорошие параметры бинарной последовательности, генерируемой с помощью правила 30, приближающиеся к параметрам «белого шума», данный метод обладает рядом недостатков с точки зрения перспективности применения КА в криптографических системах.

Первый недостаток связан с существованием возможности дешифрации потокового кода в случае, когда имеется информация о открытом тексте и любой участок потокового кода двух соседних каналов генератора на основе КА. Действительно, опираясь на основное свойство КА – локальности взаимодействий клеток (каждая клетка взаимодействует только с окружающими её соседями), можно строить системы дешифрации потоковых кодов. Например, если кроме открытого текста известен участок последовательности битов, сгенерированных соседней клеткой, то процесс нахождения значений соседних невидимых битов может производиться по следующему правилу:

$$c_{i-1} = c_i' \oplus (c_i \vee c_{i+1}). \quad (2)$$

Таким образом можно получить набор началь-

ных состояний всего массива клеток.

Второй недостаток, который мы хотели бы отметить, связан с возможностью построения алгоритма обратимости клеточных автоматов, обладающих свойством локальности взаимодействий клеток. Продемонстрируем обратимость КА на примере «правила 30». Алгоритм обратимости КА можно разделить на три циклично повторяющихся этапа:

1. Значение битов пары соседних клеток выбираются равными «0», «0»;

2. Используя формулу (2) находятся значения всех битов «обратного» массива КА;

3. Используя формулу (1) определяется несовпадение с битами «прямого» массива КА на основе «обратного». При несовпадении – переход на этап 2 (для первого раза – «0», «1»; второго – «1», «0»; третьего – «1», «1»). При совпадении – переход на этап 1.

На рис. 1 схематично продемонстрированы этапы алгоритма обратимости клеточных автоматов для массива из 8 клеток. Крестиками показаны несовпадения значений битов. Из рисунка видно, что в качестве правильного будет выбран вариант (*г*).

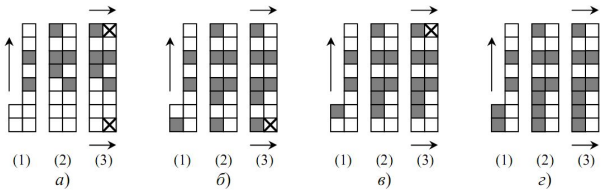

Рис. 1. Пояснение алгоритма обратимости КА

На рис. 2 – 4 приведён интересный пример, использующий свойства обратимости КА на основе «правила 30» для массива из 256 клеток.

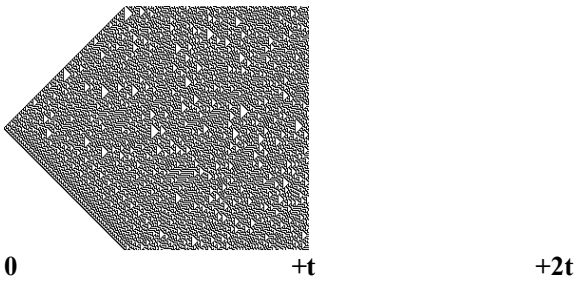

Рис. 2. Прямая генерация последовательности с единичным начальным состоянием КА

2. Модификация классических КА

Для устранения недостатков КА с точки зрения их применения в криптографических системах, в работе [7] был предложен новый класс КА, базирующийся на псевдослучайном механизме определения локализации взаимодействующих клеток.

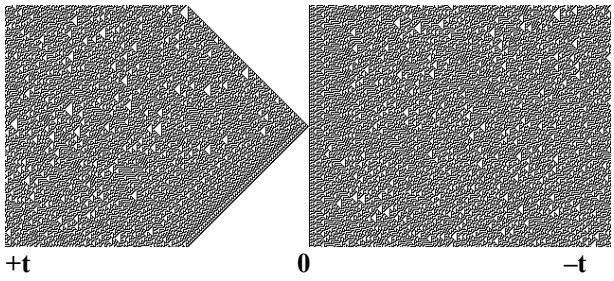

Рис. 3. Обратная генерация последовательности с состоянием КА в момент времени **+t**

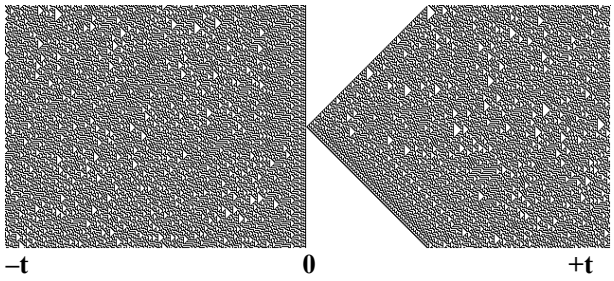

Рис. 4. Прямая генерация последовательности с состоянием КА в момент времени **–t**

В данном случае каждая клетка массива КА может взаимодействовать не строго с соседними с ней клетками, а с любыми клетками всего массива КА. Предлагается формировать номера (адреса) взаимодействующих клеток из набора битов соседних клеток. Например, для массива из 256 клеток, адрес любой клетки можно сформировать, используя $\log_2(256) = 8$ клеток. В случае, когда некоторое состояние массива КА – равновероятностный равномерно-распределённый набор битов, то адрес и состояние любой клетки в следующий момент времени будет определяться псевдослучайным образом.

Используя подобного рода подход совершенно не обязательно искать сложные правила взаимодействий КА, с помощью которых генерировались бы бинарные последовательности. Достаточно выбрать правило, удовлетворяющее условию симметричности относительно количества выходных и входных единиц или нулей, например: $\overline{c_i}$, $c_i \oplus c_j$, $\overline{c_i \oplus c_j}$, и т.д. Кроме того, данная модификация открывает возможность применения КА в качестве программных генераторов псевдослучайных чисел.

Наиболее простым способом построения быстродействующего программного генератора псевдослучайных бинарных последовательностей является непосредственное вычисление состояния очередной клетки, выдача её значения и переход к следующей соседней. Но данный способ абсолютно неприменим с точки зрения криптографии, поскольку потоковый шифр, в данном случае, полностью состоит

из «ключей», то есть полного набора состояний массива клеток. Для криптографических задач необходимо обеспечить неполную (или абсолютно непредсказуемую с точки зрения атакующего) информацию, генерируемую массивом клеточных автоматов. Можно было бы передавать в канал, например, каждый второй или третий результат взаимодействий КА, но данный подход снижает эффективность и статистические характеристики генератора.

Рассмотрим генератор на основе функции «$\oplus$», в котором переход к следующей очередной взаимодействующей клетке происходит псевдослучайным образом. В данном случае правило взаимодействия можно записать в виде:

$$c_i' = c_a \oplus c_i,\ i = i + r + s, \qquad (3)$$

где $a = \left(i + d + \sum_{k=0}^{(\log_2 n)-1} c_{i+d+k} \cdot 2^{(\log_2 n)-1-k} \right) \bmod n$ – адрес клетки, взаимодействующей с i-й клеткой;

n – общее количество клеток;

r – минимальное расстояние от i-й клетки до клетки, которая будет взаимодействовать в следующий момент времени;

s – количество единичных значений в наборе адресных клеток;

d – расстояние от i-й клетки до набора адресных клеток.

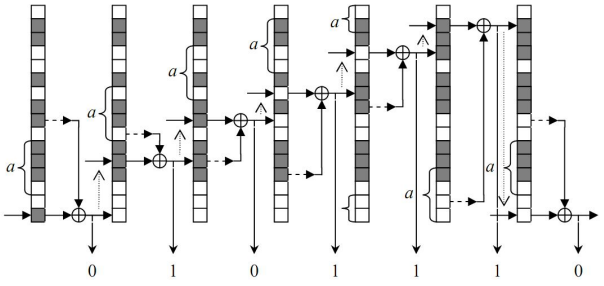

Рис. 5. Иллюстрация работы алгоритма по формуле (3) ($n = 16$, $d = 1$, $r = 1$)

3. Анализ необратимости

Несмотря на кажущуюся, на первый взгляд, криптографическую эффективность и статистически высокое качество, данный генератор не лишён недостатков. При увеличении параметров d и r генератор демонстрирует быстрый переход от хаотического поведения в упорядоченное. На рис. 6 показан случай перехода к упорядоченному поведению при зарисовке экрана размером 640*480.

Причиной такого поведения является спонтанное «сужение» количества взаимодействующих клеток массива. На рис. 7 показана зарисовка состояния массива КА через каждые 10000 взаимодействий клеток для случая, изображённого на рис. 6.

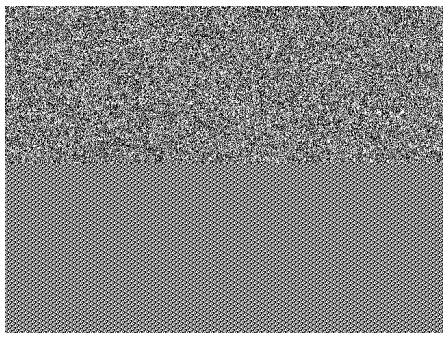

Рис. 6. Переход к упорядоченному поведению. Зарисовка 640*480. ($n = 256$, $d = 1$, $r = 3$)

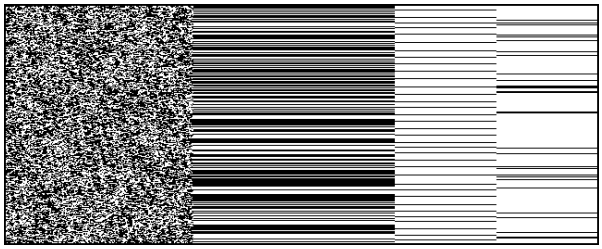

Рис. 7. Переход к упорядоченному поведению. Зарисовка состояния массива КА через каждые 10000 взаимодействий клеток. ($n = 256$, $d = 1$, $r = 3$)

Переход между рис. 7.*а* и рис. 7.*б* соответствует переходу к упорядоченному состоянию. Рис. 7.*в* соответствует «базовым» взаимодействующим клеткам (сплошные стрелки-указатели на рис. 5). Рис. 7.*г* соответствует взаимодействующим клеткам, индексы которых сформировались с помощью набора адресных клеток (пунктирные стрелки-указатели на рис. 5). Видно, что в упорядоченном режиме, позиции взаимодействующих клеток «перепрыгивают» на определённые стационарные позиции.

Такое поведение свидетельствует, кроме всего прочего, о **необратимости** бинарной последовательности, генерируемой на основе формул (3), поскольку невозможно построить алгоритм, переводящий систему от порядка к хаосу в конкретный момент времени.

При уменьшении параметров d и r генератор демонстрирует более долгий переход от хаотического поведения в упорядоченное (псевдослучайный поиск стационарных позиций). Увеличение количества клеточных массивов, как и увеличение параметров d и r, также негативно влияет на хаотическое поведение, причём с ростом количества кле-

точных массивов упорядоченность наблюдается практически с первых моментов генерации.

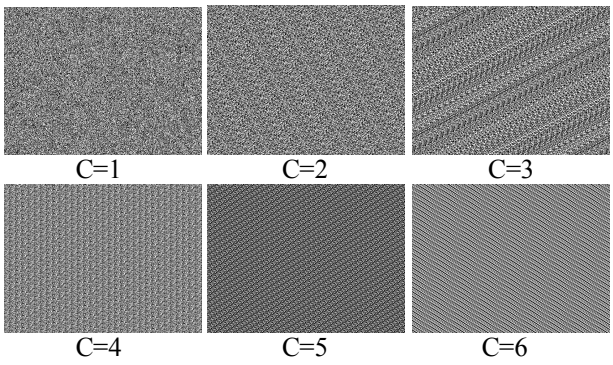

Рис. 8. Типичные картины при зарисовке экрана 640*480 для различного количества массивов клеточных автоматов C

4. Противодействие самоорганизации

Для устранения возможности перехода в упорядоченное поведение необходимо обеспечить взаимодействие как можно большего количества разных клеток за как можно меньшее количество времени. В предельном случае для количества КА – n необходимо обеспечить взаимодействие всех клеток за n шагов.

Рассмотрим генератор на основе функции «$\oplus$», в котором переход к следующей очередной взаимодействующей клетке происходит псевдослучайным образом. Полное взаимодействие всех клеток массива КА за n шагов обеспечивается с помощью некоторого массива $A[i,j]$, где $i = 0,1,2,\ldots,n-1$; $j = 1,2$. Массив содержит адреса взаимодействующих клеток, причём индексация массива происходит последовательно. В данном случае правило взаимодействия можно записать в виде:

$$c_{A[i,1]}' = c_{A[a,1]} \oplus c_{A[i+1,1]}, \quad A[i,2] \Leftrightarrow A[a,2],$$
$$i = (i+1) \bmod n, \qquad (4)$$

где $a = \left(i + 1 + \sum_{k=0}^{(\log_2 n)-1} c_{i+1+k} \cdot 2^{(\log_2 n)-1-k} \right) \bmod n$ – адрес, сформированный из значений набора адресных клеток;

n – общее количество клеток;

при i=0 столбцы адресного массива меняются местами.

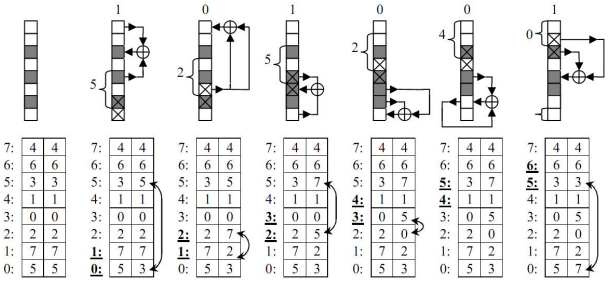

Рис. 9. Работа алгоритма по формуле (4) (n = 8)

Заключение

В статье проведены исследования обратимости программных генераторов псевдослучайных бинарных последовательностей на основе КА. Сформулированы рекомендации относительно таких модификаций существующих алгоритмов, которые гарантировали бы необратимость генерируемых ими последовательностей. Описанные алгоритмы и структуры могут быть использованы при реализации программных генераторов псевдослучайных бинарных последовательностей.

В дальнейших научных исследованиях планируется провести анализ криптографической устойчивости предложенных алгоритмов, а также реализация на их основе программных генераторов, скоростные характеристики которых не уступали бы широко распространённым на сегодняшний день генераторам.

Литература

1. Wolfram, S. Random sequence generation by cellular automata [Text] / S. Wolfram. // Advances in Applied Mathematics. – 1986. – T. 7. – P. 123-164.

2. Toffoli, T. Invertible cellular automata: a review [Text] / T. Toffoli, N. Margolus// Physica. – 1990. – T. 45. – P. 229-253.

3. Tao, R. On finite automaton public-key cryptosystem [Text] / R. Tao, S. Chen // Theoretical Computer Science. – 1999. – T. 226, No. 1-2. – P. 143-172.

4. Seredynski, F. Cellular automata computations and secret key cryptography [Text] / F. Seredynski, P. Bouvry, A. Y. Zomaya // Parallel Computing. – 2004. – T. 30, No. 5-6. – P. 753-766.

5. Singh, A. Cryptographic algorithm using cellular automata rules [Text] / A. Singh, S. Mishra // International Journal of Computer Application. – 2014. – T. 4, No. 3 – P. 57-64.

6. Advances on random sequence generation by uniform cellular automata [Text] / E. Formenti, K. Imai, B. Martin, J. Yun´es // Computing with New Resources. – 2014. – T. 17. – P. 56–70.

7. Ostapov, S. E. Investigation of Properties of Pseudorandom Binary Sequences Generator on the Basis of Cellular Automata [Text] / S. E. Ostapov,

V. V. Zhikharevich, L. Val' // 9th International Conference on Development and Application Systems, Suceava, Romania, 22-24 May 2008. – P. 115-117.

References

1. Wolfram, S. Random sequence generation by cellular automata. *Advances in Applied Mathematics*, 1986, vol. 7, pp. 123-164.

2. Toffoli, T., Margolus, N. Invertible cellular automata: a review. *Physica*, 1990, vol. 45, pp. 229-253.

3. Tao, R., Chen, S. On finite automaton public-key cryptosystem. *Theoretical Computer Science*, 1999, vol. 226, no. 1-2, pp.143-172.

4. Seredynski, F., Bouvry, P., Zomaya, A. Cellular automata computations and secret key cryptography. *Parallel Computing*, 2004, vol. 30, no. 5-6, pp.753-766.

5. Singh, A., Mishra, S. Cryptographic algorithm using cellular automata rules. *International Journal of Computer Application*, 2014, vol. 4, no. 3, pp. 57-64.

6. Formenti, E., Imai, K., Martin, B., Yun´es, J. Advances on random sequence generation by uniform cellular automata. *Computing with New Resources*, 2014, vol.17, pp. 56–70.

7. Ostapov S. E., Zhikharevich, V. V., Val', L. Investigation of Properties of Pseudorandom Binary Sequences Generator on the Basis of Cellular Automata. *Proceedings of the DAAS*, Suceava, Romania, 22-24 May 2008, pp. 115-117.

Поступила в редакцию 23.03.2016, рассмотрена на редколлегии 14.04.2016

ДОСЛІДЖЕННЯ ЗВОРОТНОСТІ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІНАРНИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

В. В. Жихаревич, С. Е. Остапов

У статті проаналізована проблема зворотності класичних клітинних автоматів, використовуваних як генератори псевдовипадкових бінарних послідовностей. Запропонована модифікація, що базується на псевдовипадковому механізмі визначення локалізації взаємодіючих клітин і забезпечує незворотність. Досліджено проблему самоорганізації динаміки генератора. Причиною такої поведінки є самовільне зменшення кількості взаємодіючих клітин масиву. Запропоновано підхід, що запобігає самоорганізації модифікованих генераторів та ґрунтується на забезпеченні взаємодії всіх клітин масиву.

Ключові слова: криптографія, клітинні автомати, зворотність.

RESEARCH OF REVERSIBILITY OF PROGRAMMATIC BINARY PSEUDORANDOM SEQUENCERS ON BASIS OF CELLULAR AUTOMATS

V. V. Zhikharevich, S. E. Ostapov

The problem of reversibility of classic cellular automats in-use as pseudorandom binary sequencers is analyzed in the article. Modification being based on the pseudorandom mechanism of determination of localization of interactive cages and providing irreversibility is offered. The problem of self-organization of the generator dynamics was investigated. The reason for this behavior is a spontaneous reduction in the number of interacting cells of the array. Modification preventing self-organization of the modified generators is offered and based on the provision of the interaction of all array cells.

Keywords: cryptography, cellular automats, reversibility.

Жихаревич Владимир Викторович – канд. физ.-мат. наук, доцент кафедры программного обеспечения компьютерных систем Черновицкого национального университета им. Ю. Федьковича, Черновцы, Украина, e-mail: vzhikhar@mail.ru.

Остапов Сергей Эдуардович – д-р физ.-мат. наук, профессор, зав. каф. программного обеспечения компьютерных систем Черновицкого национального университета им. Ю. Федьковича, Черновцы, Украина, e-mail: sergey.ostapov@gmail.com.

Zhikharevich Vladimir Victorovich – PhD of physical and mathematical sciences, associate professor of the Department of Computer Systems Software, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine, e-mail: vzhikhar@mail.ru.

Ostapov Sergey Eduardovich – Dr. Sci., Professor, head of the Department of Computer Systems Software, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine, e-mail: sergey.ostapov@gmail.com.