Наука и Образование
МГТУ им. Н.Э. Баумана
Сетевое научное издание
ISSN 1994-0408

Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 04. С. 92–105.

DOI: **10.7463/0416.0837506**

Представлена в редакцию: 09.03.2016
Исправлена: 23.03.2016

УДК 519.713+004.056.55

Исследование характеристик лавинного эффекта обобщенных клеточных автоматов на основе графов малого диаметра

Балк Е. А.[1], **Ключарёв П. Г.**[1,*]

*pk.iu8@yandex.ru

[1]МГТУ им. Н.Э. Баумана, Москва, Россия

Данная работа является продолжением цикла статей, посвященных исследованию свойств обобщенных клеточных автоматов и криптографических алгоритмов на их основе. Ее основным предметом рассмотрения являются обобщенные клеточные автоматы на основе неориентированных регулярных графов малого диаметра $D < 5$ и степени вершин $k = 3$ и $k = 4$. В статье представлено теоретическое обоснование выбора графов клеточных автоматов, в соответствии с требованиями предъявляемыми к криптографическим алгоритмам легковесной криптографии (lightweight cryptography) и особенностями архитектуры программируемых логических интегральных схем (ПЛИС). Проведено исследование пространственной и интегральной характеристик лавинного эффекта для выбранных клеточных автоматов. Результатом является экспериментальное подтверждение достаточно хороших показателей характеристик лавинного эффекта для обобщенных клеточных автоматов на основе двух семейств графов.

Ключевые слова: обобщенный клеточный автомат, шифрование, шифр, криптография

Введение

Низкая скорость выполнения операций шифрования и расшифрования – одна из основных проблем, возникающих при практической реализации криптографических алгоритмов. Одним из подходов к повышению производительности является создание параллельной реализации алгоритма. На практике это не всегда возможно, если изначально при разработке в алгоритм не закладывалась возможность такой реализации. Клеточные автоматы по своей сущности являются параллельными системами и обладают хорошими показателями характеристик лавинного эффекта и статистических свойств выходной последовательности, что делает естественным их применение в качестве базового криптографического примитива для генераторов псевдослучайных чисел, блочных шифров и криптографических хеш-функций. Эти особенности структуры позволяют создать высокоскоростную аппаратную реализацию на основе микросхем ПЛИС (Программируемых логических интегральных схем) [8].

Впервые обобщённые клеточные автоматы были использованы для генерации псевдослучайной последовательности в работе [11], это направление получило развитие в цикле статей [4-9].

В вышеуказанных работах были рассмотрены обобщенные клеточные автоматы на основе графа достаточно большого диаметра $D \geq 5$. Согласно [3], выбор графа с минимальным диаметром обеспечивает лучшие характеристики лавинного эффекта в обобщенных клеточных автоматах. Основной задачей данной статьи является исследование свойств обобщенных клеточных автоматов на основе графов с диаметром $D = 3$ и $D = 4$.

Основные понятия и определения

В данном разделе кратко приведены основные определения и понятия, относящиеся к теории обобщенных клеточных автоматов:

Обобщенным клеточным автоматом будем называть пару (G, f), где:

- $G = (V, E)$ – ориентированный мультиграф, ($V = \{v_1, \dots, v_N\}$ – множество его вершин, а E – мультимножество ребер) размера N, с каждой вершиной которого ассоциирована булева переменная, причем все вершины пронумерованы числами от 0 до $(N - 1)$. Переменную, ассоциированную с *i*-ой вершиной, обозначимm_i. Мы будем называть такие переменные *ячейками* обобщенного клеточного автомата. Для каждой вершины смежные ей вершины пронумерованы числами от 0 до $(k - 1)$ и называются *окрестностью* ячейки m_i.
- Функция $f: \{0; 1\}^k \to \{0; 1\}$ – *локальная функция связи*.

Неориентированным однородным обобщенным клеточным автоматом будем называть обобщенный клеточный автомат, у всех ячеек которого одинаковая функция связи f, т.е. для любого $i \in \{1, \dots, N\}$ выполняется $f_i = f$ и для любого ребра (u, v) в его графе существует и ребро (v, u). Граф такого автомата можно рассматривать как неориентированный, если заменить каждую пару ребер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$. Граф является регулярным. Далее будут рассматриваться только неориентированные обобщенные клеточные автоматы на основе неориентированных регулярных графов, которые для краткости мы будем называть обобщенными клеточными автоматами и графами соответственно. Степени вершин таких клеточных автоматов одинаковы: $d_1 = d_2 = \dots = d_N = d$.

Исходя из определения выше, для построения обобщенного клеточного автомата достаточно задать его граф и локальную функцию связи, которая должна быть равновесной. Для повышения линейной сложности выходной последовательности и улучшения её статистических свойств локальная функция связи должна обладать максимальной степенью нелинейности.

Принцип работы обобщенного клеточного автомата заключается в следующем:

Автомат работает по дискретным временным шагам, в начальный момент времени t_0, каждая ячейка памяти m_i имеет некоторое начальное значение $m_i(0), i = 1, \dots n$. С помощью локальной функции связи на шаге *t* вычисляются новые значения переменных:

$$m_i(t) = f\left(m_{\eta(i,0)}(t-1), m_{\eta(i,1)}(t-1), \dots, m_{\eta(i,k-1)}(t-1)\right), \quad (1)$$

где $\eta(i,1)$ – номер вершины, смежной с вершиной i и имеющей номер j.

Выходом однородного обобщенного клеточного автомата на шаге с номером t называется совокупность значений первых r ячеек: $m_0(t), m_1(t), \dots, m_r(t)$.

1. Выбор графа обобщенного клеточного автомата

Для ряда задач, таких как разработка легковесных криптографических алгоритмов предъявляются повышенные требования к количеству используемых аппаратных ресурсов. В случае ПЛИС, реализация данного требования заключается в минимизации числа задействованных логических элементов, что является важным для целого ряда приложений (например, [1,2]). Количество используемых в реализации логических элементов, в первую очередь, определяется числом входов так называемой *таблицы поиска* (LUT), представляющей из себя запоминающее устройство, которое хранит в памяти таблицу истинности булевой функции от r-переменных и осуществляющей поиск значения соответствующей булевой функции вместо непосредственного вычисления значений. В связи с тем, что наибольшее распространение получили ПЛИС с таблицей поиска на 4 и 6 входов, далее будут рассматриваться неориентированные 4- и 6-регулярные графы минимального диаметра.

Оценим максимально возможный порядок графа заданной степени вершины k и диаметра D при помощи *границы Мура* $M_{k,D}$. [13]:

$$M_{k,D} \le 1 + k + k(k-1) + \cdots k(k-1)^{D-1} =$$

$$\begin{cases} \frac{k(k-1)^D - 2}{k-2} & k \neq 2 \\ 2D+1 & k = 2 \end{cases}, \quad (2)$$

Легко заметить, что $M_{4,2} = 17$, а $M_{6,2} = 37$. В теории графов задача нахождения графа максимального порядка n по заданной степени вершин k и диаметру D называется *задачей степени/диаметра* и обозначается $\max n_{k,D}$. В настоящее время $\max n_{4,2}$=17, а $\max n_{6,2} = 32$ [12], что делает затруднительным применение автоматов на их основе в качестве генераторов псевдослучайных последовательностей. Поэтому в дальнейшем будем рассматривать графы $F_{4,3}, F_{4,4}, F_{6,3}, F_{6,4}$, для которых соответственно $M_{4,3} = 53$, $M_{4,4} = 161$, $M_{6,3} = 187$, $M_{6,4} = 937$. На сегодняшний день максимальный порядок графов согласно [12] для выбранных значений степени вершин k и диаметра D принимает следующие значения: $\max n_{4,3} = 41$, $\max n_{4,4} = 98$, $\max n_{6,3} = 111$, $\max n_{6,4} = 390$. Рассмотрим эти графы применительно к задаче построения обобщённых клеточных автоматов, обладающих хорошими характеристиками лавинного эффекта.

Граф $\max n_{4,3} = 41$ получен эвристическим методом согласно алгоритму [15]. Первоначально генерируется случайный граф G, состоящий из n вершин. После этого для уменьшения диаметра D к графу итеративно применятся вариант алгоритма Кернигана-Лина [16,17] , который удаляет 2 или более несмежных ребра и заменяет их новыми, таким образом, что граф остается регулярным. При этом множество заменяемых ребер не пересекается с множеством новых ребер, т.е. $V_o \cap V_n = \emptyset$. Это продолжается до тех пор, пока не достигнут целевой диаметр D или другие изменения невозможны.

Граф $\max n_{6,4}$=390 был впервые рассмотрен в работе [18]. Для его построения был использован вариант метода *распределения меток* (voltage assignment) [19]. Предварительно рассмотрим конечный, неориентированный граф Г, который может содержать петли, кратные ребра и *полуребра*. Полуребрами графа Г называются ребра, имеющие только одну инцидентную вершину [18]. Согласно [21], можно представить ненаправленные ребра графа Г, которые не являются полуребрами, в виде пары противоположно направленных дуг, называемых *стрелами* (darts). Пусть e – стрела, тогда обозначим e^{-1} стрелу, противоположно направленную к стреле e (т.е. $((e^{-1})^{-1}) = e$. Множество всех стрел графа обозначим $P(\Gamma)$ и т.к. каждое ребро ненаправленного графа представляется в виде пары противоположно направленных стрел, то $|P(\Gamma)|$=2$|E(\Gamma)$. Пусть T – конечная группа, тогда отображение $\alpha: P(\Gamma) \to T$ называется *распределением меток,* если $\alpha(e^{-1}) = (\alpha(e))^{-1}$ для любой стрелы $e \in P(\Gamma)$. Конечную группу T при этом называют *группой меток* (voltage group). Пара (Γ, α) называется *размеченным графом* (voltage graph) и определяет *покрывающий граф* (lift*)* Γ^{α} графа Г следующим образом: пусть V множество вершин графа Г. Тогда множество вершин и множество стрел покрывающего графа $V^{\alpha} = V(\Gamma) \times T$ и $P^{\alpha} = P(\Gamma) \times T$ соответственно.

На первоначальном этапе выбирается подходящий граф Г (степень его вершин должна быть равна степени вершин искомого графа; в случае построения графа $\max n_{6,4}$=390 использовался дипольный граф [18]) и группа меток T. Далее случайным образом происходит присваиваивание меток ребрам, петлям, и полуребрам графа Г. Согласно [18], группа меток T не является абелевой и задается как полупрямое произведение абелевых групп. В процессе работы распределение, создающее в покрывающем графе Γ^{α} петли и кратные ребра, сразу отвергается. После того как процесс построения покрывающего графа завершен, определяется его диаметр D. Если в пределах предварительно заданного количества попыток все сгенерированные распределения меток образуют покрывающие графы диаметра больше требуемого, выбирается новая группа. Если подходящее распределение найдено, то результат записывается и процедура останавливается.

Согласно [3] хорошие характеристики лавинного эффекта обобщенного клеточного автомата обеспечивают графы, обладающие как можно большим коэффициентом расширения. Задача нахождения значения коэффициента расширения является вычислительно трудной, поэтому, согласно [4], рассмотрим значение 2-го элемента спектра λ_2 выбранных графов [3].

Спектр представляет собой отсортированный по убыванию набор собственных чисел матрицы смежности графа.

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \quad (3)$$

Для выбранных графов

$\lambda_2(\max n_{4,3}) = 3{,}214, \lambda_2(\max n_{4,4}) = 3{,}339, \lambda_2(\max n_{6,3}) = 3{,}579, \lambda_2(\max n_{6,4}) = 4{,}207.$

Согласно *теореме Нили,* нижняя граница для λ_2:

$$\lambda_2 \geq 2\sqrt{k-1} - \frac{2\sqrt{k-1}-1}{D}, \quad (4)$$

где D – диаметр графа, k – степень вершины графа.

Таким образом, полученные значения λ_2, согласно (4), являются, близкими к минимальным. Это означает, что выбранные графы является хорошими расширителями среди графов такого порядка.

Характеристики лавинного эффекта для выбранных автоматов

В работах [1-7] так же было введено понятие интегральной характеристики лавинного эффекта для обобщенных клеточных автоматов.

Рассмотрим два идентичных обобщенных клеточных автомата A_1 и A_2. Обозначим векторы их ячеек соответственно $\vec{m}^{(1)} = ({m_0}^{(1)}, \ldots, {m_{n-1}}^{(1)})$ и $\vec{m}^{(2)} = ({m_0}^{(2)}, \ldots, {m_{n-1}}^{(2)})$. Вектор начального заполнения будет различаться в одном разряде. Не нарушая общности будем считать, что номер ячейки, соответствующий такому разряду, равен нулю:

$${m_0}^{(2)} = \begin{cases} {m_i}^{(1)}(0), i \neq 0 \\ \neg {m_i}^{(1)}(0)\ i = 0 \end{cases} \quad (5)$$

Интегральной характеристикой [3-9] лавинного эффекта называется зависимость от номера такта количества различающихся ячеек у двух различных в одной ячейке начальных заполнений клеточного автомата:

$$\omega(t) = \frac{1}{n}\sum_{j=0}^{n-1}\left({m_i}^{(1)}(0) \oplus {m_j}^{(2)}(t)\right) \quad (6)$$

Пространственной характеристикой лавинного эффекта назовем зависимость отношения от расстояния от вершины с номером 0 до самой дальней вершины, ячейка которой у двух автоматов не совпадает, к эксцентриситету вершины с номером 0:

$$\mu(t) = \frac{1}{e(0)} \cdot \max_{j \in \mathbb{Z}_n}((m_j^{(1)}(t) \oplus m_j^{(2)}(t)) \cdot \Delta(0,j)) \ , \quad (7)$$

$\Delta(i,j)$ – длина минимального пути из ячейки i в ячейку j, а $e(i)$ – эксцентриситет вершины графа, соответствующей ячейке i.

Очевидно, что для выбранных автоматов стоит рассматривать усредненное по достаточно большому количеству начальных заполнений значение интегральной и пространственной характеристик лавинного эффекта: $\hat{\omega}(t)$ и $\hat{\mu}(t)$. Начиная с некоторого t_n, выполняется $\hat{\omega}(t) = \omega_n$ и $\hat{\mu}(t) = \mu_n$ при $t \geq t_n$. Чтобы обеспечить хорошие статистические свойства выходной последовательности необходимо, чтобы $\omega_n = 0.5$, а $\mu = 1$, [3].

Локальную функцию связи для всех клеточных автоматов будем выбирать согласно [4]

На рисунках ниже приведены графики усредненных значений интегральных характеристик и пространственных характеристик лавинного эффекта в зависимости от номера такта для 10000 пар различных начальных заполнений, различных в одной ячейке.

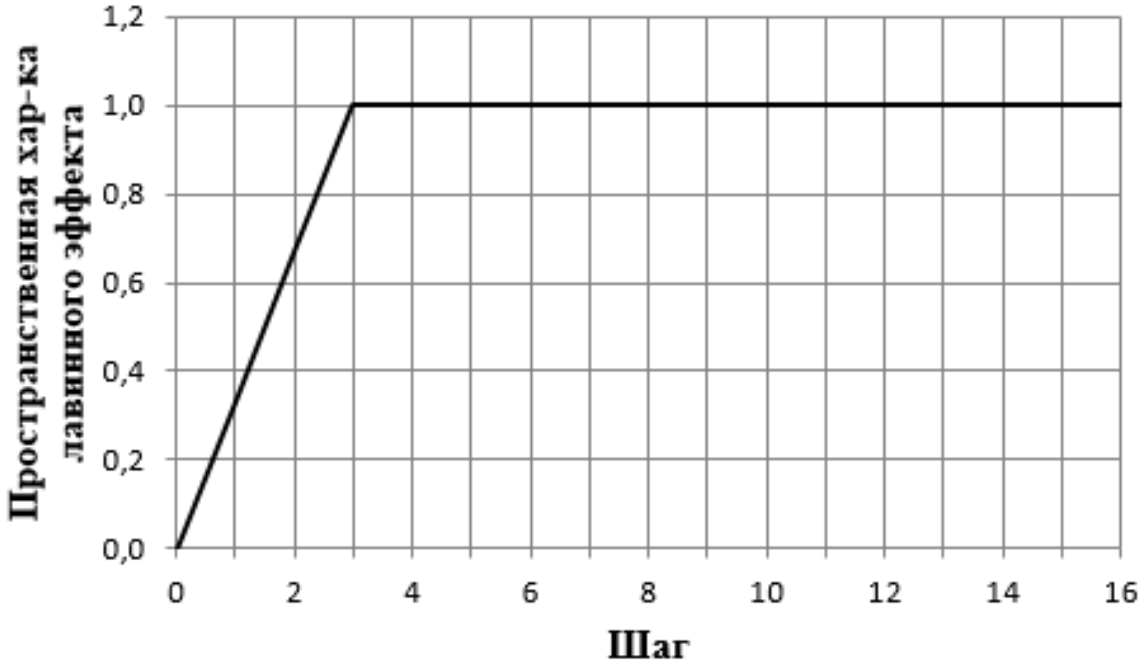

Рис. 1. Усредненная пространственная характеристика лавинного эффекта для графов $\boldsymbol{max\ n_{4,3}}$ и $\boldsymbol{max\ n_{6,3}}$.

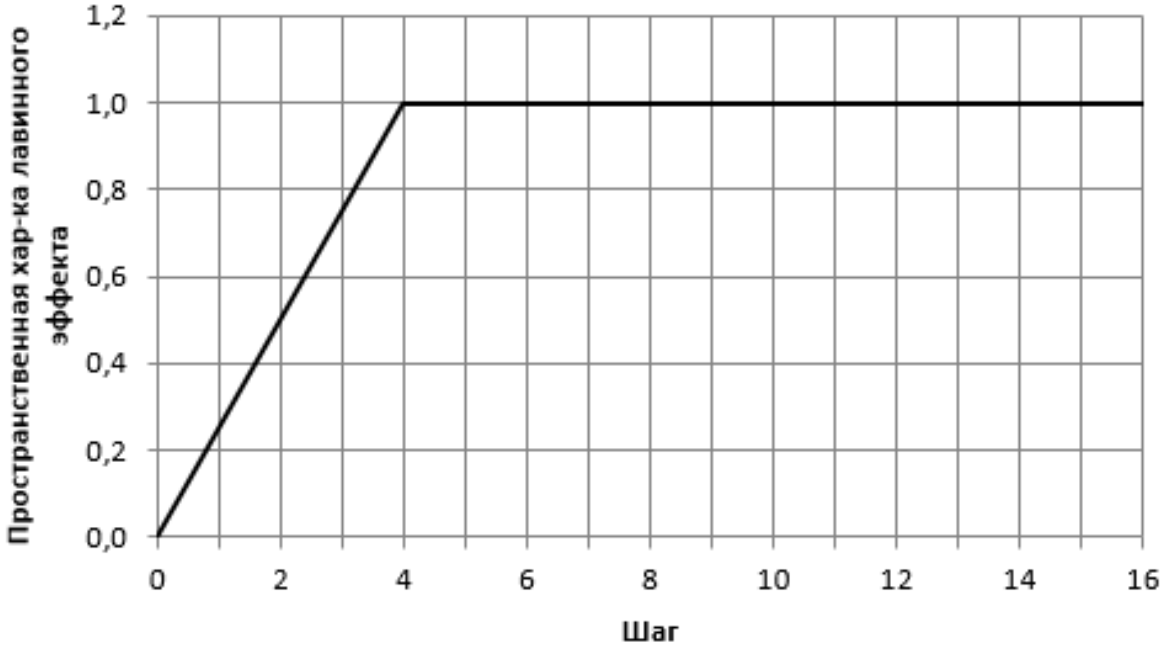

Рис. 2. Усредненная пространственная характеристика лавинного эффекта для графов $\boldsymbol{max\ n_{4,4}}$ и $\boldsymbol{max\ n_{6,4}}$.

Рис. 3. Усредненная интегральная характеристика лавинного эффекта для графа $\boldsymbol{max\ n_{4,3}}$

Рис. 4. Усредненная интегральная характеристика лавинного эффекта для графа $\boldsymbol{max\ n_{4,4}}$

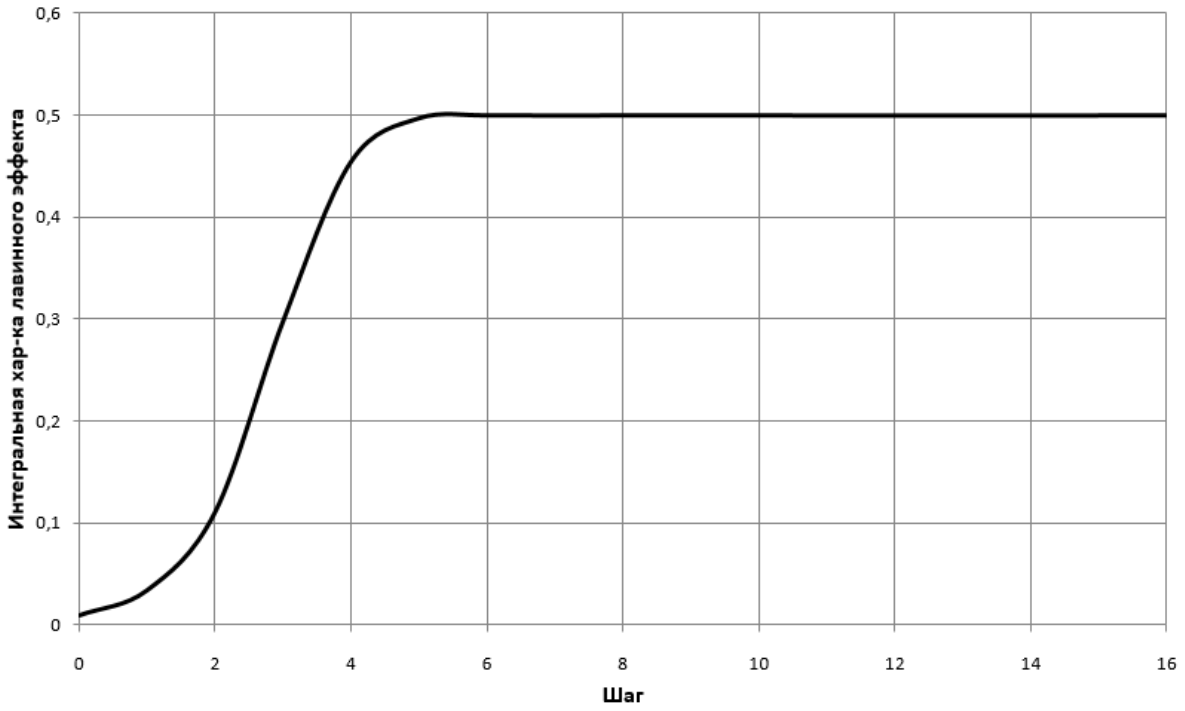

Рис. 5. Усредненная интегральная характеристика лавинного эффекта для графа $\boldsymbol{max\ n_{6,3}}$

Рис. 6. Усредненная интегральная характеристика лавинного эффекта для графа $\boldsymbol{max\ n_{6,4}}$

Полученные результаты в целом подтверждают результаты [14]. Для графов клеточных автоматов малого размера $max\ n_{4,3}$ и $max\ n_{4,4}$ несмотря на малый диаметр выбранного графа и небольшое значение коэффициента λ_2, не получила подтверждение гипотеза

значении $t_n \approx$ D. Из графиков видно, что для графов $max\ n_{4,3}$ и $max\ n_{4,4}$ смена значений ячеек для $t_n = 10$ происходит для примерно 47% ячеек. Само значение t_n =10, значительно превосходит значение диаметра, что говорит о недостаточно хороших рассеивающих свойствах автомата. Это может быть связано с малым порядком выбранных графов и малым размером окрестности автомата. В работах [10,11] были получены схожие значения интегральной характеристики лавинного эффекта для обобщенных клеточных автоматов большего размера с окрестностью 4.

Обобщенный клеточный автомат на основе графа $max\ n_{6,3}$ показал хорошие характеристики лавинного эффекта уже при $t_n = 5$. Достаточно малый порядок графов $F_{6,3}$ и хорошие характеристики лавинного эффекта позволяют использовать их в легковесной криптографии, например, для создания S-блоков симметричных блочных шифров и базового примитива для генераторов псевдослучайных последовательностей.

Обобщенный клеточный автомат на основе графа $max\ n_{6,4}$ показал хорошие значения характеристик лавинного эффекта при $t_n = 7$ и может быть использован в качестве основы для генератора псевдослучайных последовательностей, псевдослучайной функции или в качестве базового примитива для алгоритма блочного шифрования в дальнейших исследованиях.

Заключение

Таким образом, все рассмотренные в рамках работы обобщенные клеточные автоматы обладают хорошими характеристики лавинного эффекта, позволяющими их использовать в качестве базовых примитивом для криптографических алгоритмов в дальнейших исследованиях. Графы с диаметром $D = 3, D = 4$ и степенью вершин $k = 6$, помимо хороших значений характеристик лавинного эффекта, так же характеризуются малым значением величины t_n, что может быть полезно в случаях, когда количество тактов работы не должно сильно превосходить t_n (например в случаях использования обобщенных клеточных автоматов в качестве блоков нелинейной замены блочных алгоритмов шифрования). Перспективным направлением исследований является изучение свойств обобщенных клеточных автоматов, у которых локальные функции связи для всех ячеек различны. Это предположительно позволяет решить проблему случаев, когда начальное заполнение ячеек является тривиальным (т.е все ячейки заполнены «0» или «1»), или близким к нему (в данном случае будет наблюдаться существенное ухудшение характеристик выходной последовательности), т.к не будет происходит сохранения значений ячеек или синхронной смены на противоположные и позволит улучшить характеристики лавинного эффекта обобщенного клеточного автомата.

Работа выполнена при частичной финансовой поддержке РФФИ, в рамках научного проекта № 16-07-00542 а.

Список литературы

1. Быков А.Ю., Панфилов Ф.А., Ховрина А.В. Алгоритм выбора классов защищенности для объектов распределенной информационной системы и размещения данных по объектам на основе приведения оптимизационной задачи к задаче теории игр с непротивоположными интересами // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 1. С. 90-107. DOI: 10.7463/0116.0830972
2. Быков А.Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015. № 9. С. 160-187. DOI: 10.7463/0915.0812283
3. Ключарев П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011. № 10. Режим доступа: http://technomag.bmstu.ru/file/504895.html?__s=1 (дата обращения 01.03.2016).
4. Ключарев П.Г. Обеспечение криптографических свойств обобщенных клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 3. Режим доступа: http://technomag.bmstu.ru/file/505222.html?__s=1 (дата обращения 01.03.2016).
5. Ключарев П.Г. О вычислительной сложности некоторых задач на обобщенных клеточных автоматах // Безопасность информационных технологий. 2012. № 1. С. 30-32. Режим доступа: http://pvti.ru/data/file/bit/2012_1/part_4.pdf (дата обращения 01.03.2016).
6. Ключарев П.Г. О периоде обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 02. Режим доступа: http://technomag.bmstu.ru/file/505165.html?__s=1 (дата обращения 01.03.2016).
7. Ключарев П.Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 01. С. 161-172. DOI: 10.7463/0113.0534640
8. Ключарев П.Г. Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 10. С. 299-314. DOI: 1013.0624722
9. Ключарев П.Г. Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 01. С. 214-223. DOI: 10.7463/0114.0675812
10. Сухинин Б.М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование. МГТУ им.

Н.Э. Баумана. Электрон. журн. 2010. № 08. Режим доступа: http://technomag.bmstu.ru/file/504603.html?__s=1 (дата обращения 01.03.2016).
11. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2010. № 9. Режим доступа: http://technomag.edu.ru/file/504604.html?__s=1 (дата обращения 01.03.2016).
12. Comellas F., Delorme C. The (degree, diameter) problem for graphs // Государственный университет Каталонии: сайт. Режим доступа: http://www-ma4.upc.es/~comellas/delta-d/taula_delta_d.html (дата обращения 15.02.2016).
13. Miller M., Širan J. Moore graphs and beyond: A survey of the degree / diameter problem // The Electronic Journal of Combinatorics. 2005. No. DS14. Режим доступа: http://www.emis.ams.org/journals/EJC/Surveys/ds14.pdf (дата обращения 01.03.2016).
14. Балк Е.А., Ключарев П.Г. Исследование характеристик лавинного эффекта неориентированных обобщенных клеточных автоматов малого размера // XI Международная научно-практическая конференция «Перспективы развития информационных технологий»: сб. матер. Новосибирск, 2013.
15. Allwright J. New (Δ, D) graphs discovered by heuristic search // Discrete Applied Mathematics. 1992. Vol. 37-38. P. 3-8. DOI: 10.1016/0166-218X(92)90120-Y
16. Lin S., Kernighan B.W. An efficient heuristic procedure for partitioning graphs // The Bell System Technical Journal. 1970. Vol. 49, no. 2. P. 291-307. DOI: 10.1002/j.1538-7305.1970.tb01770.x
17. Lin S., Kernighan B.W. An Effective Heuristic Algorithm for the Traveling-Salesman Problem // Operations Research. 1973. Vol. 21, no. 2. P. 498-516. DOI: 10.1287/opre.21.2.498
18. Loz E., Širan J. New record graphs in the degree-diameter problem // Australasian Journal of Combinatorics. 2008. Vol. 41. P. 63-80. Режим доступа: http://ajc.maths.uq.edu.au/pdf/41/ajc_v41_p063.pdf (дата обращения 01.03.2016).
19. D McKay B., Miller M., Širan J. A Note on Large Graphs of Diameter Two and Given Maximum Degree // Journal of Combinatorial Theory, Series B. 1998. Vol. 74, no. 1. P. 110-118. DOI: 10.1006/jctb.1998.1828
20. Dinneen M.J., Hafner P.R. New results for degree/diameter problem // Networks. 1994. Vol. 24, no. 7. P. 359-367. DOI: 10.1002/net.3230240702
21. Brankovic L., Miller M., Plesnik J., Ryan J., Širan J. Large graphs with small degree and diameter: A voltage assignment approach // Australasian Journal of Combinatorics. 1998. No. 18. P. 65-76. Режим доступа: http://ajc.maths.uq.edu.au/pdf/18/ajc-v18-p65.pdf (дата обращения 01.03.2016).

Science & Education of the Bauman MSTU
Electronic journal
ISSN 1994-0408

Science and Education of the Bauman MSTU, 2016, no. 04, pp. 92–105.

DOI: **10.7463/0416.0837506**

Received: 09.03.2016
Revised: 23.03.2016

Small Diameter Graph-based Investigation of Avalanche Effect Characteristics of Generalized Cellular Automata

E.A. Balk[1], **P.G. Klyucharev**[1,*]

*pk.iu8@yandex.ru

[1]Bauman Moscow State Technical University, Moscow, Russia

Keywords: generalized cellular automata, cipher, cryptography

This article is sequel to a series of articles concerning with the study of generalized cellular automata and their cryptographic properties. It, mainly, focuses on using the generalized cellular automata, as the basic cryptographic primitives, according to requirements for algorithms of the so-called lightweight cryptography. One of the main requirements is to minimize the hardware resources used. According to this requirement, in case of using a FPGA algorithm for hardware implementation, the paper offers to consider only generalized cellular automata based on the regular graphs of degree k = 4 and k = 6 because their efficient hardware implementations widely practise the FPGA with 4- and 6-input look-up. To construct the generalized cellular automata were used graphs with diameter D = 3 and D = 4 because the generalized cellular automata based on the regular graphs of small diameter have good characteristics of the avalanche effect and the Moore boundary places restrictions on the maximum order of graph for a specified degree value of the graph and diameter.

The findings of the research results for the cellular automata based on the maximum order of graphs with diameter D = 3 and D = 4 and the degree of the vertex k = 4 are broadly consistent with previous results for generalized automata in vicinity of 4. They are characterized by quite a large, regarding a diameter of the graph, value of the number of cycles from the start of operating automata till its reaching the maximum value of the integral avalanche effect characteristics.

According to the research results, the selected cellular automata-based graphs with diameter D = 3 and D = 4 and the vertex degree k = 6 have shown good values of the avalanche effect characteristics and possess good scattering properties.

Thus, all the abovementioned generalized cellular automata have good characteristics of the avalanche effect, and can be used as the basic cryptographic primitives. A promising research area is to create the non-uniform cellular automata, which have different local communication functions for all the cells.

References

1. Bykov A.Yu., Panfilov F.A., Khovrina A.V. The Algorithm to Select Security Classes for Objects in Distributed Information Systems and Place Data in the Objects Through Reducing the Optimization Problem to the Theory of Games with Non-conflicting Interests. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2016, no. 1, pp. 90-107. DOI: 10.7463/0116.0830972 (in Russian).
2. Bykov A.Yu., Shmatova E.S. The Algorithms of Resource Distribution for Information Security Between Objects of an Information System Based on the Game Model and Principle of Equal Security of Objects. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2015, no. 9, pp. 160-187. DOI: 10.7463/0915.0812283 (in Russian).
3. Klyucharev P.G. Cellular automations based on Ramanujan graphs in the field of the generation of pseudorandom sequences. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2011, no. 10. Available at: http://technomag.bmstu.ru/file/504895.html?__s=1 , accessed 01.03.2016. (in Russian).
4. Klyucharev P.G. On cryptographic properties of generalized cellular automation. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 3. Available at: http://technomag.bmstu.ru/file/505222.html?__s=1 , accessed 01.03.2016. (in Russian).
5. Klyucharev P.G. On computational complexity of some problems on generalized cellular automata. *Bezopasnost Informatsionnykh Tekhnology*, 2012, no. 1, pp. 30-32. Available at: http://pvti.ru/data/file/bit/2012_1/part_4.pdf , accessed 01.03.2016. (in Russian).
6. Klyucharev P.G. On period of generalized cellular automation. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 02. Available at: http://technomag.bmstu.ru/file/505165.html?__s=1 , accessed 01.03.2016. (in Russian).
7. Klyucharev P.G. Cryptographic hash functions based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU,* 2013, no. 01, pp. 161-172. DOI: 10.7463/0113.0534640 (in Russian).
8. Klyucharev P.G. Performance and effectiveness of hardware realization of stream ciphers based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU,* 2013, no. 10, pp. 299-314. DOI: 1013.0624722 (in Russian).
9. Klyucharev P.G. Implementation of cryptographic hash functions based on generalized cellular automata, based FPGAs: performance and efficiency. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2014, no. 01, pp. 214-223. DOI: 10.7463/0114.0675812 (in Russian).
10. Sukhinin B.M. The Analysis of Avalanche Effect Characteristics in Binary Cellular Automata with Balanced Transition. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science*

and Education of the Bauman MSTU, 2010, no. 08. Available at: http://technomag.bmstu.ru/file/504603.html?__s=1 , accessed 01.03.2016. (in Russian).

11. Sukhinin B.M. The Development of Pseudorandom Binary Sequences Generators Based on Cellular Automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2010, no. 9. Available at: http://technomag.edu.ru/file/504604.html?__s=1 , accessed 01.03.2016. (in Russian).
12. Comellas F., Delorme C. *The (degree, diameter) problem for graphs*. State University of Catalonia: website. Available at: http://www-ma4.upc.es/~comellas/delta-d/taula_delta_d.html , accessed 15.02.2016.
13. Miller M., Širan J. Moore graphs and beyond: A survey of the degree / diameter problem. *The Electronic Journal of Combinatorics*, 2005, no. DS14. Available at: http://www.emis.ams.org/journals/EJC/Surveys/ds14.pdf , accessed 01.03.2016.
14. Balk E.A., Klyucharev P.G. Research of characteristics of avalanche effect undirected generalized cellular automats of small size. *11 Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Perspektivy razvitiya informatsionnykh tekhnologii": sb. mater.* [Collection of materials of the11th International scientific-practical conference "Prospects of development of information technologies"]. Novosibirsk, 2013. (in Russian, unpublished).
15. Allwright J. New (Δ, D) graphs discovered by heuristic search. *Discrete Applied Mathematics*, 1992, vol. 37-38, pp. 3-8. DOI: 10.1016/0166-218X(92)90120-Y
16. Lin S., Kernighan B.W. An efficient heuristic procedure for partitioning graphs. *The Bell System Technical Journal*, 1970, vol. 49, no. 2, pp. 291-307. DOI: 10.1002/j.1538-7305.1970.tb01770.x
17. Lin S., Kernighan B.W. An Effective Heuristic Algorithm for the Traveling-Salesman Problem. *Operations Research*, 1973, vol. 21, no. 2, pp. 498-516. DOI: 10.1287/opre.21.2.498
18. Loz E., Širan J. New record graphs in the degree-diameter problem. *Australasian Journal of Combinatorics*, 2008, vol. 41, pp. 63-80. Available at: http://ajc.maths.uq.edu.au/pdf/41/ajc_v41_p063.pdf , accessed 01.03.2016.
19. D McKay B., Miller M., Širan J. A Note on Large Graphs of Diameter Two and Given Maximum Degree. *Journal of Combinatorial Theory, Series B,* 1998, vol. 74, no. 1, pp. 110-118. DOI: 10.1006/jctb.1998.1828
20. Dinneen M.J., Hafner P.R. New results for degree/diameter problem. *Networks*, 1994, vol. 24, no. 7, pp. 359-367. DOI: 10.1002/net.3230240702
21. Brankovic L., Miller M., Plesnik J., Ryan J., Širan J. Large graphs with small degree and diameter: A voltage assignment approach. *Australasian Journal of Combinatorics*, 1998, no. 18, pp. 65-76. Available at: http://ajc.maths.uq.edu.au/pdf/18/ajc-v18-p65.pdf , accessed 01.03.2016.