Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ОБОБЩЕННЫХ КЛЕТОЧНЫХ АВТОМАТОВ

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Медведева Сергея Алексеевича

Научный руководитель
профессор, д.ф.-м.н. В.А. Молчанов

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

Последовательности псевдослучайных чисел широко применяются в различных областях – от компьютерного программирования, имитационного моделирования и методов Монте-Карло до криптографии. При этом качество получаемых в процессе работы результатов напрямую зависит от свойств используемых псевдослучайных последовательностей.

В настоящее время задача построения генераторов псевдослучайных последовательностей с заданными вероятностными распределениями настолько актуальна, что стали появляться научно-производственные предприятия, специализирующиеся на генерации больших последовательностей псевдослучайных чисел (см., например, [1],[2]).

Большинство алгоритмов генерации псевдослучайных чисел обладают различными недостатками, такими, как например: низкая скорость генерации, предсказуемость выходной последовательности, короткий период, сложность реализации и т. д. Поэтому важной задачей является разработка генераторов, которые обладают хорошими статистическими свойствами и сочетают в себе высокую производительность и способность генерировать псевдослучайные последовательности.

Целью выпускной квалификационной работы является разработка методов генерации псевдослучайных последовательностей с помощью обобщенных клеточных автоматов. В работе рассматриваются следующие задачи:

1) применение обобщенных клеточных автоматов для построения генераторов псевдослучайных последовательностей;

2) построение обобщенных клеточных автоматов с помощью регулярных графов;

3) разработка методов построения регулярных графов (в частности, графов Рамануджана);

4) тестирование генераторов псевдослучайных последовательностей, построенных с помощью обобщенных клеточных автоматов.

В первом разделе приводятся основные понятия и свойства классических и обобщенных клеточных автоматов.

Во втором разделе описываются методы построения генераторов псевдослучайных последовательностей на основе классических одномерных и двумерных клеточных автоматов.

Третий раздел посвящен рассмотрению методов построения графов Любоцкого-Филипса-Сарнака, способов формирования на их основе генераторов псевдослучайных последовательностей, построенных с помощью обобщенных клеточных автоматов.

В четвертом разделе производится анализ и сравнение результатов работы генератора псевдослучайных последовательностей на основе обобщенных клеточных автоматов и результатов работы других генераторов. Далее рассматриваются различные конфигурации генератора на основе обобщенных клеточных автоматов и выбирается наиболее оптимальная из них.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе приводятся основные понятия и свойства классических и обобщенных клеточных автоматов.

Обобщенным клеточным автоматом размера *n* называется пара (G, f), где $f: \{0;1\}^k \to \{0;1\}$ – локальная функция связи, а $G = (V, E)$ – ориентированный регулярный мультиграф (V – множество вершин, а E – мультимножество дуг), с каждой вершиной которого ассоциирована булева переменная. Такие переменные называются ячейками.

Выходом обобщенного клеточного автомата на шаге с номером t являются значения первых r ячеек: $m_0(t), m_1(t), \dots, m_{r-1}(t)$. Соответственно, последовательность

$$m_0(t_0),\ m_1(t_0),\ \dots,\ m_{r-1}(t_0),\ m_0(t_0+1),\ m_1(t_0+1), \dots, m_{r-1}(t_0+1), \dots$$

называется выходной последовательностью клеточного автомата.

Неориентированным обобщенным клеточным автоматом называется обобщённый клеточный автомат (G, f), где граф $G = (V, E)$ такой, что для любого $(u, v) \in E$ существует $(v, u) \in E$.

Во втором разделе описываются методы построения генераторов псевдослучайных последовательностей на основе классических одномерных и двумерных клеточных автоматов.

Одномерные клеточные автоматы представляют собой последовательность ячеек a_i, которые могут принимать значения от 0 до $(k-1)$ в зависимости от r ячеек справа и слева от текущей. Значения ячеек изменяются синхронно в дискретные моменты времени по определенному правилу:

$$a_i' = f(a_{i-r}, a_{i-r+1}, \dots, a_{i+r}).$$

Среди всего множества правил построения одномерных клеточных автоматов существуют два, наиболее подходящих для генерации псевдослучайных чисел. Эти правила нелинейны и задаются следующим образом:

$$a_i' = a_{i-1}\ XOR\ (a_i\ OR\ a_{i+1})$$

или, что тоже самое,

$$a_i' = (a_{i-1} + a_i + a_{i+1} + a_i a_{i+1})\ mod\ 2$$

(называется правило 30) и

$$a_i' = a_{i-1}\ XOR\ (a_i\ OR\ (NOT\ a_{i+1}))$$

или, что то же самое,

$$a_i' = (1 + a_{i-1} + a_{i+1} + a_i a_{i+1})\ mod\ 2$$

(называется правило 45).

В частности в качестве одномерных клеточных автоматов выступают автоматы, построенные с помощью правила 30.

В качестве классического двумерного клеточного автомата рассматриваются автоматы с двумерной решеткой. Окрестность каждой ячейки автомата состоит из всех ячеек, смежные с ней.

Рассматриваемые генераторы псевдослучайных чисел были реализованы программно на языке C++. Исходные коды программ приведены в приложениях Б и В.

Третий раздел посвящен рассмотрению методов построения графов Любоцкого-Филипса-Сарнака.

Расширяющим графом называется неориентированный регулярный мультиграф G, такой, что $h(G) \geq c$, где c – некоторая константа, а $h(G)$ – коэффициент расширения, определяемы следующим образом:

$$h(G) = \min_{\{S \subset V,\ 0<|S|\leq \frac{|V|}{2}\}} \frac{|\partial(S)|}{|S|},$$

где $\partial(S)$ – множество ребер, каждое из которых инцидентно ровно одной вершине из множества S [16].

Графом Рамануджана называется такой расширяющий граф, для которого выполняется неравенство

$$\lambda_2 \leq 2\sqrt{k-1}.$$

Степенью нелинейности булевой функции f называется число $\deg(f)$ переменных в самом длинном слагаемом её полинома Жегалкина. Функция f

называется аффинной, если $\deg(f) = 1$. Бент-функцией называется булева функция с чётным числом переменных, для которой расстояние Хэмминга [28] от множества аффинных булевых функций с тем же числом переменных максимально. Другими словами, бент-функция обладает максимальной степенью нелинейности [37].

Одно из семейств графов Рамануджана – графы Любоцкого-Филипса-Сарнака (LPS-графы) [23],[24]. Существует два метода построения таких графов: метод на основе проективной группы и метод на основе проективной прямой.

В подразделе 3.1 описывается метод на основе проективной группы, а в подразделе 3.2 – метод на основе проективной прямой. Далее приводится способ формирования генераторов псевдослучайных последовательностей, построенных с помощью обобщенных клеточных автоматов методом на основе проективной прямой.

Генератор псевдослучайных последовательностей на основе обобщенных клеточных автоматов построенный методом на основе проективной прямой был реализован программно на языке C++. Исходный код программы приведен в приложении Г.

Для ускорения работы генератора псевдослучайных последовательностей на основе обобщенного клеточного автомата реализовано параллельное вычисление на модулях видеокарты. Модификация написана на языке PyOpenCL под управлением CUDA. Исходный код программы приведен в приложении Д.

В четвертом разделе производится анализ и сравнение результатов работы генератора псевдослучайных последовательностей на основе обобщенных клеточных автоматов и результатов работы других генераторов.

Здесь исследуются различные конфигурации генераторов псевдослучайных последовательностей на основе обобщенных клеточных автоматов и выделяются наиболее оптимальные из них.

Проверка полученных последовательностей осуществлялась с помощью набора статистических тестов DieHard [40] и NIST [45][46], каждый из которых

определяет отклонение полученных характеристик генератора псевдослучайных последовательностей от ожидаемых характеристик генератора случайных последовательностей с равномерным распределением.

Рассматриваемые модификации генераторов псевдослучайных чисел были реализованы программно на языке C++. Исходные коды программ приведены в приложениях Ж и И.

ЗАКЛЮЧЕНИЕ

В работе рассмотрены возможности применения обобщенных клеточных автоматов для построения генераторов псевдослучайных последовательностей. Реализован алгоритм генерации регулярных графов Любоцкого-Филипса-Сарнака (семейство графов Рамануджана), на базе которых построены обобщенные клеточные автоматы, являющиеся основой для генераторов псевдослучайных последовательностей. Тестирование результатов работы данного генератора показало, что полученные на его основе последовательности по своим характеристикам являются близкими к случайным двоичным последовательностям с равномерным распределением.

Построенные в работе обобщенные клеточные автоматы имеют близкие к оптимальным характеристики лавинного эффекта. Генераторы псевдослучайных последовательностей, основанные на таких клеточных автоматах, вырабатывают последовательности, имеющие статистические свойства высокого криптографического качества, что подтверждается успешным прохождением набора тестов DieHard и NIST. Такие генераторы могут найти применения как в криптографии и стеганографии, так и в различных областях математического моделирования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. RANDOM.ORG—True Random Number Service [Электронный ресурс] / RANDOM.ORG [Электронный ресурс]. URL: http://www.random.org (дата обращения 20.10.2015). Загл. с экрана Яз. англ.

2. HotBits: Genuine Random Numbers, Generated by Radioactive Decay [Электронный ресурс] / Index Librorum Liberorum [Электронный ресурс]. URL: http://www.fourmilab.ch/hotbits (дата обращения 13.09.2015). Загл. с экрана Яз. англ.

3. Computation in artificially evolved, non-uniform cellular automata . Sipper M., Tomassini M. [Электронный ресурс] / Google [Электронный ресурс]. URL: http://www.sciencedirect.com/science/article/pii/S0304397598001510 (дата обращения 24.09.2015). Загл. с экрана Яз. англ.

4. Non-Uniform Cellular Automata Cattaneo G. [Электронный ресурс] / Springer LINK [Электронный ресурс]. URL: http://link.springer.com/chapter/10.1007%2F978-3-642-00982-2_26 (дата обращения 18.09.2015). Загл. с экрана Яз. англ.

5. Stream Cyphers with One- and Two-Dimensional Cellular Automata Tomassini M., Perrenoud M. [Электронный ресурс] / Google [Электронный ресурс]. URL: https://books.google.ru/books?id=9E_nwkCXX7oC&pg=PA286&lpg=PA286&dq=0M.%2C%20and%20TwoDimensional%20Cellular%20Automata&f=false (дата обращения 24.09.2015). Загл. с экрана Яз. англ.

6. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов Сухинин Б.М. [Электронный ресурс] / Науки и образование [Электронный ресурс]. URL: http://technomag.edu.ru/doc/159565.html. (дата обращения 29.09.2015). Загл. с экрана Яз. рус.

7. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов Сухинин Б.М.

[Электронный ресурс] / Науки и образование [Электронный ресурс]. URL: http://technomag.edu.ru/doc/ 159714.html. (дата обращения 29.09.2015). Загл. с экрана Яз. рус.

8. Cellular Automata Wolfram S. [Электронный ресурс] / Stephen Wolfram [Электронный ресурс]. URL: http://www.stephenwolfram.com/publications/ academic/?cat=cellular-automata (дата обращения 12.09.2015). Загл. с экрана Яз. англ.

9. A New Kind of Science Wolfram S. [Электронный ресурс] / WOLFRAMSCIENCE [Электронный ресурс]. URL: http://www.wolframscience.com/nksonline/toc.html (дата обращения 15.11.2015). Загл. с экрана Яз. англ.

10. Random Sequence Generation by Cellular Automata Wolfram S. [Электронный ресурс] / Stephen Wolfram [Электронный ресурс]. URL: http://www.stephenwolfram.com/publications/academic/random-sequence-generation-cellular-automata.pdf (дата обращения 12.09.2015). Загл. с экрана Яз. англ.

11. Cryptography with Cellular Automata Wolfram S. [Электронный ресурс] / Stephen Wolfram [Электронный ресурс]. URL: http://www.stephenwolfram.com/ publications/academic/cryptography-cellular-automata.pdf (дата обращения 12.09.2015). Загл. с экрана Яз. англ.

12. Repeating Rule 30 patterns [Электронный ресурс] / I write, therefore I am [Электронный ресурс]. URL: http://www.iwriteiam.nl/Rule30.html (дата обращения 02.09.2015). Загл. с экрана Яз. англ.

13. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов Сухинин Б.М. [Электронный ресурс] / Прикладная дискетная математика [Электронный ресурс]. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid =pdm&paperid=180&option_lang=rus (дата обращения 20.11.2015). Загл. с экрана Яз. англ.

14. On Moore graphs with diameter 2 and 3 Hoffman A., Singleton R. [Электронный ресурс] / ACM Digital Library [Электронный ресурс]. URL: http://dl.acm.org/ citation.cfm?id=1661219 (дата обращения 13.09.2015). Загл. с экрана Яз. англ.

15. Moore graphs and beyond: A survey of the degree/diameter problem Miller M., Širán J. [Электронный ресурс] / The Electronic Journal of Combinatorics [Электронный ресурс]. URL: http://www.combinatorics.org/ojs/index.php /eljc/article/viewFile/DS14/pdf (дата обращения 15.09.2015). Загл. с экрана Яз. англ.

16. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей Ключарёв П.Г. [Электронный ресурс] / Наука и образование [Электронный ресурс]. URL: http://technomag.edu.ru/doc/241308.html (дата обращения 10.10.2015). Загл. с экрана Яз. рус.

17. Экспандеры: конструкции и приложения А.Е. Ромащенко [Электронный ресурс] / Кафедра дискретной математики ФИВТ МФТИ [Электронный ресурс]. URL: http://ru.discrete-mathematics.org/?page_id=1293 (дата обращения 02.10.2015). Загл. с экрана Яз. рус.

18. Лекции по алгебре: Учебное пособие для вузов Фаддеев Д. К. [Электронный ресурс] / Научная библиотека [Электронный ресурс]. URL: http://stu.sernam.ru/lect_alg.php (дата обращения 25.09.2015). Загл. с экрана Яз. рус.

19. Expander graphs and their applications Shlomo Hoory, Nathan Linial, Avi Widgerson [Электронный ресурс] / Computer Science and Engineering: The Hebrew University of Jerusalem [Электронный ресурс]. URL: http://www.cs.huji.ac.il/~nati/PAPERS/expander_survey.pdf (дата обращения 20.11.2015). Загл. с экрана Яз. англ.

20. SPECTRAL GRAPH THEORY Chung F.R.K [Электронный ресурс] / UCSD Mathematics [Электронный ресурс]. URL: http://www.math.ucsd.edu/~fan/ research/revised.html (дата обращения 10.09.2015). Загл. с экрана Яз. англ.

21. Методы вычислений Березин И. С., Жидков Н. П. [Электронный ресурс] / Научная библиотека [Электронный ресурс]. URL: http://info.alnam.ru/book_calc2.php (дата обращения 25.09.2015). Загл. с экрана Яз. рус.

22. Some Applications of Modular Forms Sarnak P. [Электронный ресурс] / Google [Электронный ресурс]. URL: https://books.google.ru/books/about/Some_ Applications_of_Modular_Forms.html?id=CRiAEnmE_DcC&redir_esc=y (дата обращения 25.09.2015). Загл. с экрана Яз. англ.

23. Явные теоретико-групповые конструкции комбинаторных схем и их применения в построении расширителей и концентраторов Маргулис Г.А. [Электронный ресурс] / Проблемы передачи информации [Электронный ресурс]. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi& paperid= 686&option_lang=rus (дата обращения 01.10.2015). Загл. с экрана Яз. рус.

24. Ramanujan graphs Lubotzky A., Phillips R., Sarnak P. [Электронный ресурс] / Springer LINK [Электронный ресурс]. URL: http://link.springer.com/article/ 10.1007%2FBF02126799 (дата обращения 20.09.2015). Загл. с экрана Яз. англ.

25. Toeplitz and Circulant Matrices: A Review, R. M. Gray [Электронный ресурс] / Stanford Engineering [Электронный ресурс]. URL: http://ee.stanford.edu/~gray/toeplitz.pdf (дата обращения 25.11.2015). Загл. с экрана Яз. англ.

26. Конечные поля Лидл Р., Нидеррайтер Г. [Электронный ресурс] / Научная литература [Электронный ресурс]. URL: http://booksshare.net/index.php?id1=4&category=physics&author=lidl-r&book=1988 (дата обращения 25.11.2015). Загл. с экрана Яз. рус.

27. On certain arithmetical functions, Ramanujan S. [Электронный ресурс] / Srinivasa Ramanujan [Электронный ресурс]. URL: http://ramanujan.sirinudi.org/Volumes/published/ram18.pdf (дата обращения 26.11.2015). Загл. с экрана Яз. англ.

28. Extremal graph theory, Bollobas B. [Электронный ресурс] / Department of Mathematical Sciences [Электронный ресурс]. URL: http://www.math.cmu.edu/~bbol/docs/math/mop2009/graph-theory-extremal.pdf (дата обращения 26.11.2015). Загл. с экрана Яз. англ.

29. Теория графов, Оре О.[Электронный ресурс] / Department of Mathematical Sciences [Электронный ресурс]. URL: http://www.math.cmu.edu/~bbol/docs/math/mop2009/graph-theory-extremal.pdf (дата обращения 26.11.2015). Загл. с экрана Яз. рус.

30. Modern graph theory, Bollobas B. [Электронный ресурс] / Springer [Электронный ресурс]. URL: https://www.springer.com/us/book/9780387984889 (дата обращения 26.11.2015). Загл. с экрана Яз. англ.

31. Regulare Graphen gegenebener Teillenweite mit Minimaler Knoten-zahl, Erdõs P., Sachs H. [Электронный ресурс] / MATHÉMATIQUE [Электронный ресурс]. URL: http://mathematique.hautetfort.com/paul-erdos-papers/ (дата обращения 26.11.2015). Загл. с экрана Яз. англ.

32. Explicit constructions of graphs without short cycles and low density codes, Margulis G. A. [Электронный ресурс] / Springer Link [Электронный ресурс]. URL: http://link.springer.com/article/10.1007%2FBF02579283 (дата обращения 27.11.2015). Загл. с экрана Яз. англ.

33. Explicit constructions of graphs without short cycles, Imrich W. [Электронный ресурс] / Springer Link [Электронный ресурс]. URL: http://link.springer.com/article/10.1007%2FBF02579157 (дата обращения 27.11.2015). Загл. с экрана Яз. англ.

34. Ramanujan Topologies for Decision Making in Sensor Networks Kar S., Moura J.M.F. [Электронный ресурс] / Electrical and Computer Engineering [Электронный ресурс]. URL: http://users.ece.cmu.edu/~moura/papers/allerton06-kar.pdf (дата обращения 09.09.2015). Загл. с экрана Яз. англ.

35. Обеспечение криптографических свойств обобщенных клеточных автоматов Ключарёв П.Г. [Электронный ресурс] / Наука и образование [Электронный ресурс]. URL: http://technomag.edu.ru/doc/358973.html (дата обращения 10.10.2015). Загл. с экрана Яз. рус.

36. Криптографические свойства нелинейных булевых функций Агафонова И.В. [Электронный ресурс] / Яндекс [Электронный ресурс]. URL: https://docviewer.yandex.ru/?url=ya-serp%3A2F%2Fdha.spb.ru%2FPDF%2FcryptoBOOLEAN.pdf&name=cryptoBOOLEAN.pdf&c=56251ea7d7c7&page=1 (дата обращения 05.10.2015). Загл. с экрана Яз. рус.

37. Нелинейные булевы функции: бент-функции и их обобщения Токарева Н. Н. [Электронный ресурс] / Институт математики им. С.Л.Соболева [Электронный ресурс]. URL: http://math.nsc.ru/~tokareva/mon/11-lap-book.pdf (дата обращения 03.10.2015). Загл. с экрана Яз. рус.

38. On “bent” functions Rothaus O. S. [Электронный ресурс] / ScienceDirect [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/pii/ 0097316576900248 (дата обращения 10.10.2015). Загл. с экрана Яз. англ.

39. Cryptographic Boolean functions and applications Cusick T. [Электронный ресурс] / Google [Электронный ресурс]. URL: https://books.google.ru/books?id=OAkhkLSxxxMC&pg=PA213&lpg=PA213&dq=Cusickq=Cusick%20T.%2C%20Cryptographic%20Boolean%20functions%20and%20applications&f=false (дата обращения 15.09.2015). Загл. с экрана Яз. англ.

40. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness [Электронный ресурс] / THE FLORIDA STATE

UNIVERSITY [Электронный ресурс]. URL: http://stat.fsu.edu/pub/diehard (дата обращения 15.10.2015). Загл. с экрана Яз. англ.

41. Robert G. Brown's General Tools Page [Электронный ресурс] / DUKE University [Электронный ресурс]. URL: http://www.phy.duke.edu/~rgb/General/dieharder.php (дата обращения 18.10.2015). Загл. с экрана Яз. англ.

42. Теория вероятностей и математическая статистика, Кремер Н.Ш. [Электронный ресурс] / IQ Академия [Электронный ресурс]. URL: http://iqacademy.ru/files/knigi/teorver&matstat/kremer_n_sh_teoriya_veroyatnostey_i_matematicheskaya_statist.pdf (дата обращения 30.11.2015). Загл. с экрана Яз. рус.

43. Producing the graphs of Lubotzky Phillips and Sarnak in Matlab, Elzinga R. [Электронный ресурс] / Department of Mathematics and Statistics [Электронный ресурс]. URL: http://www.mast.queensu.ca/~ctardif/lps/LPSSup.pdf (дата обращения 30.11.2015). Загл. с экрана Яз. англ.

44. Основы кодирования, Вернер М. [Электронный ресурс] / Сахара: Микроконтроллеры [Электронный ресурс]. URL: http://caxapa.ru/thumbs/409009/Osnovy_kodirovaniya__M._VERNER_.pdf (дата обращения 30.11.2015). Загл. с экрана Яз. рус.

45. A Statistical Test Suite for Random and Pseudorandom Numer Generators for Cryptographic Applications [Электронный ресурс] / NIST: Computer Security Division_Computer Security Resource Center [Электронный ресурс]. URL: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (дата обращения 7.12.2015). Загл. с экрана Яз. англ.

46. Statistical Testing of Random Number Generators, Soto J. [Электронный ресурс] / NIST: Computer Security Division_Computer Security Resource Center [Электронный ресурс]. URL: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf (дата обращения 7.12.2015). Загл. с экрана Яз. англ