КЛЕТОЧНЫЕ АВТОМАТЫ В КРИПТОГРАФИИ. Часть 1

Жуков А.Е.[1]

Клеточные автоматы – одна из старейших моделей вычислений, насчитывающая уже более 70 лет. Появившаяся в конце 40-х годов XX века, теория клеточных автоматов дала множество теоретических и практических приложений в виде вычислительных моделей для различных природных феноменов и явлений. Клеточные автоматы – вездесущи и повсеместны. Они – самостоятельные объекты теоретического изучения, они же – инструмент для моделирования в науке и технике. В основе популярности клеточных автоматов лежит их сравнительная простота в сочетании с большими возможностями для моделирования совокупности взаимосвязанных однородных объектов. Кроме того, клеточные автоматы, являясь параллельными структурами, прекрасно подходят для моделирования дискретных параллельных процессов, для создания параллельных алгоритмов обработки информации и представляют интерес в качестве основы вычислительной техники с высокопараллельной архитектурой.

Ключевые слова*: клеточно-автоматная модель, множество конечных автоматов, регулярная решётка, окрестность фон Неймана, алгебраическая разрешимость, криптосистема, история конечных автоматов*

DOI: 10.21681/2311-3456-2017-3-70-76

Немного истории

> «… клеточные автоматы изобретались много раз под разными названиями, и несколько отличающиеся друг от друга понятия употреблялись под одним и тем же названием».
>
> *Т. Тоффоли, Н. Марголус [1]*

Более или менее полная история возникновения и развития теории клеточных автоматов (КлА), а также обзор их возможных приложений требует отдельной и весьма объемистой статьи. Читателю, заинтересованному историей клеточных автоматов, можно предложить обзоры [2, 3] и книги [1, 4-8]. Здесь же мы ограничимся самыми общими историческими сведениями.

Наиболее известным и распространенным мнением является то, что создателем клеточных автоматов является Джон фон Нейман. Более внимательное изучение истории появления этого понятия показывает, что в конце 40-х годов идея клеточного автомата что называется «витала в воздухе» и к числу его «создателей» следует причислить по крайней мере пятерых выдающихся ученых.

В 1940-е годы Джон фон Нейман (János Lajos Neumann, 1903–1957), будучи сотрудником Лос-Аламосской национальной лаборатории, работал над теорией самовоспроизводящихся систем [4, 7]. В это же время другой сотрудник той же лаборатории, Станислав Улам (Stanisław Marcin Ulam, 1909–1984), разрабатывал математическую модель роста кристаллов [9]. Обмен идеями между коллегами привел к возникновению клеточно-автоматной модели эволюции систем.

Приблизительно тогда же работавшие в Массачусетском Технологическом Институте (MIT) Норберт Винер (Norbert Wiener, 1894–1964) и Артуро Розенблют (Arturo Rosenblueth, 1900–1970) разработали клеточно-автоматную модель возбудимой среды для описания распространения импульсов в нервных узлах [10].

Пятым «отцом» теории клеточных автоматов следует считать выдающегося немецкого инженера Конрада Цузе (Konrad Zuse, 1910–1995) – создателя первого в современном смысле программируемого компьютера Z3 (1941 г.) и первого языка программирования высокого уровня (1945 г.). Клеточные автоматы (под именем «вычисляющих пространств») рассматривались им в качестве возможной архитектуры вычислительных систем. В силу понятных политических и идеологических соображений Конрад Цузе не получил всемирной славы как «отец кибернетики» что, однако, не умаляет его заслуг.

В 1969 году К. Цузе опубликовал книгу «Вычислимый космос» [11], где выдвинул предположение, что по своей природе Вселенная является гигантским клеточным автоматом, а происходящие в ней физические процессы – суть производимые вычисления. В то время такой взгляд на Вселенную был шокирующим, тогда как сейчас идея вычисляющей саму себя Вселенной получила дальнейшее развитие [6, 8, 12-17]. Книга К.Цузе положила начало так называемой «цифровой физике» – модному ныне направлению, относящемуся не столько к современной физике, сколько к философии.

Первая же фундаментальная книга, посвященная непосредственно клеточным автоматам, была создана по черновым записям и незавершенным статьям

1 Алексей Евгеньевич Жуков, кандидат физико-математических наук, доцент, директор ассоциации «РусКрипто» – Российского отделения IACR (Международной Ассоциации Криптологических Исследований), Москва. E-mail: aez_iu8@rambler.ru

Дж. фон Неймана, законченным и переработанным его многолетним сотрудником А. Бёрксом (Burks A.W.) и вышла в свет в 1966 г. [7].

Классические клеточные автоматы

Клеточные автоматы являются простыми моделями пространственно протяженных децентрализованных систем, состоящих из большого числа однородных составляющих компонент (клеток, ячеек), а внутреннее функционирование сводится к локальному взаимодействию между соседними компонентами [1, 8, 18-30].

Классический клеточный автомат представляет собой упорядоченный набор ячеек памяти, образующих некоторую регулярную *n*-мерную решетку (на практике наибольшее распространение приобрели клеточные автоматы небольшой размерности – с одно- или двумерными решетками). Структура пространственной решетки зависит от формы входящих в нее ячеек. Так, например, в двумерном случае можно рассматривать ячейки прямоугольной, треугольной, шестиугольной формы (рис. 1); разумеется, возможны и иные варианты. Наибольшее внимание получили клеточные автоматы, в которых ячейки имеют квадратную форму, а сами решетки – прямоугольную.

Каждая ячейка памяти клеточного автомата может хранить одно значение из некоторого конечного множества (как правило – 1 бит). Время для клеточного автомата изменяется дискретными шагами (тактами). Смена значений всех ячеек решетки происходит синхронно и одновременно при увеличении номера такта в соответствии с правилами перехода, определяющими новое значение каждой ячейки памяти как функцию от текущих значений соседних ячеек.

Таким образом, для классических клеточных автоматов выполняются свойства:

- **Параллельность вычислений.** Классический клеточный автомат представляет собой дискретную динамическую систему с параллельным вычислением значений ячеек памяти;
- **Свойство локальности.** Значение каждой ячейки памяти на следующем такте работы клеточного автомата зависит только от текущих значений ячеек в некоторой ее окрестности (и, возможно, от значения самóй рассматриваемой ячейки);
- **Свойство однородности.** Решетка однородна. Правила перехода являются одинаковыми для всех ячеек клеточного автомата.

Математически клеточный автомат над множеством Ω с d-мерной решеткой размера $X_1 \times X_2 \times \ldots \times X_d$, окрестностью Ψ и локальной функцией связи $f: \Omega^{|\Psi|} \to \Omega$, задающей правила перехода, определяется как конечный автономный автомат $\boldsymbol{A}(S, s_0, F)$, где:

$S = \Omega^{X_1 \cdot X_2 \cdot \ldots \cdot X_d}$ – множество внутренних состояний автомата;

$s_0 \in S$ – начальное состояние автомата;

$F: S \to S$ – функция переходов, определяет следующее состояние автомата как функцию от текущего состояния.

При этом множество внутренних состояний S представляет собой всевозможные заполнения d-мерной решетки ячеек памяти элементами множества Ω, каждое внутреннее состояние $s \in S$ автомата $\boldsymbol{A}$ соответствует некоторому заполнению ячеек памяти, а функция переходов F определяется через локальную функцию связи $f: \Omega^{|\Psi|} \to \Omega$, когда новое заполнение каждой ячейки памяти определяется текущим заполнением ячеек, образующих ее окрестность.

В некоторых моделях решетка клеточного автомата считается бесконечной. Тогда считается, что все ячейки, кроме конечного числа, имеют в начальный момент «пустое» (нулевое) заполнение. Однако в большинстве приложений решетка клеточного автомата имеет конечные размеры. В этом случае возникает так называемая «проблема краевых клеток» – как задавать значения функции для ячеек, у которых отсутствует часть соседей. Чаще всего в соответствии со свойством однородности для разрешения проблемы краевых клеток противоположные края решетки клеточных автоматов отождествляются. Тогда одномерные клеточные автоматы можно пред-

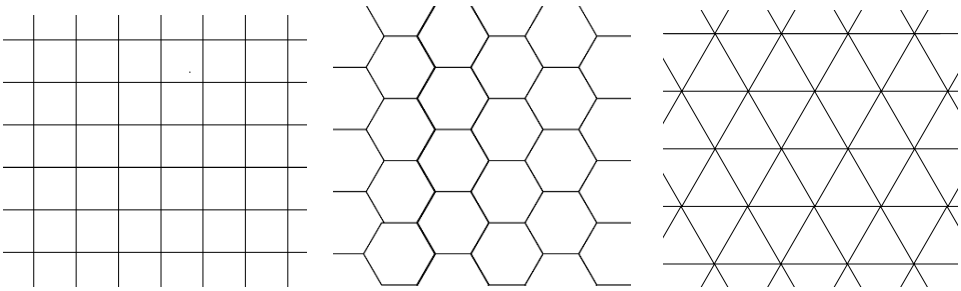

***Рис. 1** – Двумерные решетки*

ставлять в виде набора ячеек памяти, объединенных в кольцо, решетку же двумерных автоматов принято отождествлять с тором (рис. 2). Реже – вводится так называемая «нулевая граница» (null-boundary): значения для отсутствующих соседей полагаются равными нулю. Известны и другие варианты решения проблемы краевых клеток.

Автомат фон Неймана

Как указывалось выше, задача, которую в 40-х годах решал фон Нейман, состояла в исследовании возможности создания самовоспроизводящихся автоматов. В процессе решения он установил тесную связь самовоспроизводящихся автоматов с машиной Тьюринга – абстрактной логической конструкцией, предложенной Аланом Тьюрингом (Alan Mathison Turing, 1912–1954) в качестве идеализированной модели вычислителя. Машину Тьюринга можно представить себе в виде устройства, способного находиться в конечном числе внутренних состояний, снабженного бесконечной внешней памятью и набором инструкций, позволяющих в зависимости от данных, записанных во внешней памяти, менять свои внутренние состояния, переходить от одной ячейки памяти к другой, меняя, при необходимости, их содержание. Машины Тьюринга с разными наборами инструкций способны к выполнению различных задач. Достоинством машин Тьюринга является простота их устройства, однако они совершенно неэффективны даже для простейших вычислений и представляют интерес исключительно с теоретической точки зрения. Так очень важным обстоятельством является тот теоретический факт, что существует машина Тьюринга, которая способна эмулировать работу любой другой машины Тьюринга, включая саму себя. Это – так называемая универсальная машина Тьюринга и она способна выполнять любые вычисления, которые выполнимы в принципе.

В 1952 г. фон Нейману удается решить проблему самовоспроизводящихся автоматов и построить соответствующий пример [7]. Автомат фон Неймана представляет собой двумерный клеточный автомат с квадратными ячейками памяти, организованными в прямоугольную решетку, окрестность каждой клетки состоит из нее самой и четырех клеток, имеющих с ней общие границы (окрестность фон Неймана). Ячейка памяти, соответствующая клетке, может находиться в 29 возможных состояниях (включая состояние, называемое «состоянием покоя»). Двумерное пространство считается бесконечным, и все клетки, кроме конечного числа, первоначально находятся в «покоящемся» состоянии. Автомат задается определенным правилом взаимодействия клеток (локальной функцией связи) и конкретной исходной конфигурацией – начальным заполнением клеток.

«Самовоспроизведение» автомата фон Неймана выражается в том, что через некоторое время после начала работы на решетке присутствуют две его точные копии, в той же конфигурации, как это было в начале работы. Сам автомат сложен, для его задания требуется порядка 200 000 ячеек. Автомат фон Неймана содержит универсальный конструктор и универсальную машину Тьюринга (универсальный вычислитель), т.е. способен выполнять любые вычисления. Хотя этот автомат никогда не был реализован на практике, главный итог состоял в том, что было доказано отсутствие логического противоречия в понятии самовоспроизводящейся машины и продемонстрировано, что самовоспроизведение не нуждается в каких-то сверхъестественных средствах.

С тех пор как фон Нейман впервые сконструировал свой автомат, многие другие исследователи либо улучшили его оригинальную конструкцию, либо разработали альтернативные конструкции. Так в 1968 г. Кодд (Codd E.F.) упростил конструкцию фон Неймана (в которой ячейки принимают 29 возможных состояний) и построил КлА с теми же свойствами, в котором каждая ячейка может принимать 8 состояний [19]. В 1971 г. Бэнкс (Banks E.R.) [31] предложил

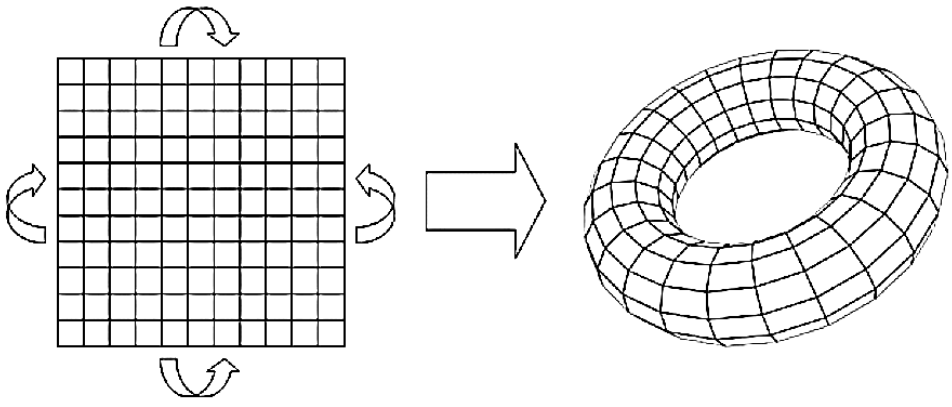

Рис. 2 *– Отождествление противоположных краев решетки двумерного клеточного автомата*

аналогичный автомат, ячейки которого могли принимать 4 состояния (см. также работы Мура (Moore E.F.) [32] и Бёркса [4]). В 1984 г. Лэнгтон (Langton C.) опубликовал самовоспроизводящийся клеточный автомат, состоящий из 86 клеток, принимающих 8 состояний, который, правда, не проявляет свойства универсального вычислителя, как это делали автоматы фон Неймана и Кодда, а просто воспроизводит сам себя [33].

Обзор пятидесятилетнего периода исследований по самовоспроизведению автоматов можно найти в статье Сиппера (Sipper M.) [34], а также в более ранних книгах Беркса и Кодда [4, 19].

Дальнейшее развитие

Начиная с 60-х годов шло активное изучение клеточных автоматов как динамических систем. Обзор результатов, полученных в этом направлении, можно найти в работе Хедлунда (Hedlund G.A.) [35].

В 70-е годы широкую известность получил двумерный клеточный автомат, известный как игра «Жизнь» (Game of Life). Игра «Жизнь» была создана в 1970 году Джоном Конвеем (Conway J.), математиком из Кембриджского университета и получила широкую известность после публикаций статей Мартина Гарднера (Gardner M.) в журнале *Scientific American* [36-37], см. также [38]. Исходным мотивом для создания игры «Жизнь» была попытка построить математическую модель для изучения реальных процессов, происходящих при зарождении, развитии и гибели популяции живых организмов. В 1982 г. удалось получить конфигурацию клеток (состояние), способную к самовоспроизведению. Дж. Конвей также доказал, что игра «Жизнь», как и самовоспроизводящийся автомат фон Неймана, имеет мощность универсальной машины Тьюринга: любая программа, которая может быть запущена на машине Тьюринга, может быть выполнена с помощью игры «Жизнь» с соответствующей первоначальной конфигурацией состояний. Эта первоначальная конфигурация кодирует и входные данные, и саму программу, которая будет обрабатывать входные данные.

Вообще исследованию вычислительных возможностей клеточных автоматов посвящен большой цикл работ (см., например, [20, 26, 39-42]). То, что клеточные автоматы могут моделировать машины Тьюринга и, следовательно, быть универсальными вычислителями, стало ясно после того, как как фон Нейман построил свой автомат, который эмулировал работу универсальной машины Тьюринга. Спустя 20 лет Смит (Smith III, A.R.) доказал, что элементарный одномерный КлА с окрестностью радиуса 1 эквивалентен машине Тьюринга [43, 44]. Заметим, кстати, что моделирование работы машины Тьюринга клеточным автоматом немедленно влечет за собой доказательство неразрешимости ряда вопросов, связанных с поведением КлА.

Интерес к КлА еще больше усилился в начале 80-х годов после того, как физик Стивен Вольфрам (Wolfram S.) опубликовал в 1983 г. первую из серии статей, исследующих различные классы клеточных автоматов [45]. В следующие 3 года он публикует работы [46-50], делающие его известным благодаря тем идеям, которые в них развиваются. В этих работах Вольфрам делает акцент на возможности использования клеточных автоматов в качестве математических моделей физических, биологических и вычислительных систем. Аргументами служат простота их конструкции, способность к сложному поведению, а также возможность точного математического анализа их поведения [51]. В 2002 году Вольфрам публикует 1280-страничную монографию «Новый тип науки» (A New Kind of Science [52]), где наглядно демонстрирует, что клеточные автоматы, будучи достаточно простой структурой, в процессе своего функционирования могут моделировать сложное поведение совокупности различных, порой весьма сложно устроенных взаимосвязанных однородных объектов.

Нельзя сказать, что идея клеточных автоматов «перевернула мир», но она по факту нашла применение почти во всех областях современной науки. Свидетельством тому – впечатляющее количество ежегодно происходящих крупных международных конференций, посвященных КлА и смежным областям:

- International Conference on Cellular Automata for Research and Industry (ACRI) – с 1994 г.
- International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA) – с 1995 г.
- International Conference «Advances in Information Technology» (IAIT)
- International Conference «Network and Parallel Computing» (NPC)
- International Conference on Unconventional Computation (UC)

Сейчас теория КлА является установившейся научной дисциплиной с многочисленными приложениями в очень многих областях науки ([5, 18, 53-67]). Вольфрам упоминает более 10 000 статей, ссылающихся его оригинальные работы по этому вопросу. Будучи математическим объектом, клеточные автоматы применимы не только в математике. Они играют важную роль в качестве моделей пространственно-распределенных динамических систем, поскольку изначально обладают рядом фундаментальных свойств, присущих физическому миру: параллелизмом, однородностью, локальностью взаимодействия. Другие

свойства, такие как обратимость и законы сохранения, могут быть обеспечены надлежащим выбором локальных функций связи. Не удивительно, что КлА успешно применяются при моделировании сложных систем в биохимии и генетике, компьютерных технологиях и информатике, экономике и социологии. Это имитационное моделирование физических процессов и систем (моделирование течения жидкости, моделирование диффузионных процессов, модель Изинга), моделирование в теории хаоса и теории фракталов, биологические модели взаимодействующих клеточных систем, включая модели самовоспроизводства, моделирование городской транспортной сети и модели структурной лингвистики. Сюда же можно отнести исследования в области искусственного интеллекта, работы по созданию новых перспективных архитектур высокопроизводительной вычислительной техники, по использованию клеточных автоматов для обработки изображений и в теории помехоустойчивого кодирования. Применяются они и в криптографии [66, 67].

Продолжение следует.

Рецензент: *Марков Алексей Сергеевич, доктор технических наук, профессор МГТУ им.Н.Э.Баумана, Москва, E-mail: a.markov@bmstu.ru*

Литература

1. Toffoli T., Margolus N. Cellular automata machines: A new environment for modeling. – Cambridge, Mass.: MIT Press, 1987. [Рус. перевод: Тоффоли Т., Марголус Н. Машины клеточных автоматов: пер. с англ. – М.: Мир, 1991.]
2. Sarkar P. A brief history of cellular automata // ACM Computing Surveys. – 2000. – vol. 32, No. 1. - P. 80–107.
3. Sutner K. Classification of cellular automata // Encyclopedia of Complexity and Systems Science. – Springer, 2009.
4. Burks A.W. Essays on cellular automata. – Urban, IL: University of Illinois Press, 1970.
5. Mainzer K. Thinking in complexity. The computational dynamics of matter, mind, and mankind. – Berlin: Springer, 2007.
6. Mainzer K., Chua L. The Universe as automaton. – Springer, 2012. – 112 p.
7. Von Neumann, J. Theory of self-reproducing automata (edited and completed by A.W. Burks). – Urbana, IL: University of Illinois Press, 1966. – 388 p. [Рус. перевод: фон Нейман Дж. Теория самовоспроизводящихся автоматов: пер. с англ. – М.: Мир, 1971].
8. Schiff J.L. Cellular automata. A Discrete View of the World. – A John Wiley & Sons Inc., Publication. University of Auckland. – 2008. – 279 p.
9. Ulam S. On some mathematical problems connected with patterns of growth of figures // Proceedings of Symposia in Applied Mathematics. – 1962. – 14. - P. 215–224.
10. Wiener N., Rosenbluth A. The mathematical formulation of the problem of conduction of impulses in a network of connected excitable elements, specifically in cardiac muscle // Arch. Inst. Cardiol. Mex. – 1946. – 16. - P. 205–265.
11. Zuse K. Rechnender Raum. – Braunschweig: Friedrich Vieweg & Sohn, 1969. [Англ. перевод: Zuse K. Calculating Space. – Cambridge, Mass.: MIT Technical Translation, 1970.]
12. Berthold O. Computational universes. – Berlin: Humboldt Universitat zu Berlin, Institut fur Informatik, 2009. – 22 p.
13. Flake G.W. The computational beauty of Nature. – MIT Press, 1998.
14. Gernert D. Cellular automata and the concept of space, Becker J., Eisele I., Mündemann, F. (eds.) Parallelism, Learning, Evolution: Proceedings of the Workshop on Evolutionary Models and Strategies/Proceedings of the Workshop on Parallel Processing: Logic, Organization, and Technology (WOPPLOT 89). – LNAI vol. 565. – Springer-Verlag, 1989. - P. 94–102.
15. Ilachinski A. Cellular automata: A discrete Universe (2nd ed.) – World Scientific Publ. Co., 2002.
16. Kauffman S.A. At home in the Universe: The search for laws of self-organization and complexity. – Oxford: Oxford University Press, 1995.
17. Petrov P. Church-Turing thesis as an immature form of Zuse-Fredkin thesis // 3rd WSEAS International Conference on Systems Theory and Scientific Computation. Special session on cellular automata and applications. – 2003. URL: http://digitalphysics.org/Publications/Petrov/Pet02a2/Pet02a2.htm
18. Chaudhuri P.P., Chowdhury D.R., Nandi S., Chattopadhyay S. Additive cellular automata, theory and applications, vol. 1. – John Wiley & Sons, 1997.
19. Codd E.F. Cellular automata // ACM Monograph series. – New York & London: Academic Press, Inc., 1968.
20. Delorme M., Mazoyer J. Cellular automata: A parallel model // Mathematics and Its Applications, vol. 460. – Kluwer Academic Publishers, 1999.
21. Ganguly N., Sikdar B.K., Deutsch A., Canright G., Chaudhuri P.P. A survey on cellular automata. – 2004. URL: http://www.cs.unibo.it/bison/publications/CAsurvey.pdf
22. Griffeath D., Moore C. New Constructions in Cellular Automata. – Oxford University Press, 2003.
23. Kari J. Theory of cellular automata: a survey // Theoretical Computer Science. – 2005. – 334. - P. 3–33.
24. Kari J. Cellular automata. Lecture notes. – University of Turku, Finland, 2016. URL: http://users.utu.fi/jkari/ca2016/
25. Preston Jr. K., Duff M.J.B. Modern cellular automata: Theory and applications. – Plenum Press, 1984.
26. Rozenberg, G., Baeck, T., Kok, J. (eds.) Handbook of Natural Computing. – Berlin: Springer, 2011.
27. Schiff J.L. Introduction to cellular automata. URL: http://psoup.math.wisc.edu/pub/Schiff_CAbook.pdf
28. Toffoli T., Margolus N. Invertible cellular automata: a review // Physica D. – 1990. – 45, 1-3. - P. 229–253.
29. Vivien H. An introduction to cellular automata. – 2003. URL: https://www.irif.fr/~yunes/ca/archives/bookvivien.pdf
30. Кудрявцев В.Б., Подколзин А.С., Болотов А.А. Основы теории однородных структур. – М.: Наука, 1990.
31. Banks E.R. Information and Transmission in Cellular Automata // Ph.D. diss. – Massachusetts Institute of Technology, 1971.
32. Moore E.F. Machine models of self-reproduction // Proceedings of Symposia in Applied Mathematics. – 1962. – 14. - P. 17–33. [Рус. перевод: Мур Э.Ф. Математические модели самовоспроизведения. В кн.: Математические проблемы в биологии: пер. с англ. – М.: Мир, 1966].
33. Langton C. Self-reproduction in cellular automata // Physica D. – 1984. –10. - P. 135–144.
34. Sipper M. Fifty years of research on self-replication: An overview // Artificial Life. – 1998. – 4. - P. 237–257.
35. Hedlund G. Endomorphisms and automorphisms of shift dynamical systems // Math. Systems Theory. – 1969. – 3. - P. 320–375.
36. Gardner M. Mathematical games: The fantastic combinations of John Conway›s new solitaire game «Life» // Scientific American. – 1970. – 223. - P. 120–123.
37. Gardner M. On cellular automata, self-reproduction, the Garden of Eden and the game of Life // Scientific American. – 1971. – 224. - P. 112–117.
38. Гарднер М. Математические досуги. – М.: Мир, 1972.
39. Mitchell M. Computation in cellular automata: A selected review // Gramss T., Bornholt S., Gross M., Mitchell M., Pellizzari T. (eds.) NonStandard Computation. – Weinheim: Wiley-VCH, 1998. - P. 95–140.

40. Morita K., Harao M. Computation Universality of one dimensional reversible injective cellular automata // IEICE Trans. – 1989. – E 72. - P. 758–762.
41. Ollinger N. Universalities in cellular automata; a (short) survey // Durand B. (ed.) Proceedings JAC 2008. – 2008. - P. 102–118.
42. Toffoli T. Computation and construction universality of reversible cellular automata // Journal of Computer and System Sciences. – 1977. – 15, №2. - P. 213–231.
43. Smith III A. Cellular automata complexity trade-offs // Inf. Control. – 1971. – 18. - P. 466–482.
44. Smith III A. Introduction to and survey of polyautomata theory // Automata, Languages, Development. – Amsterdam: North-Holland Publishing Co., 1976.
45. Wolfram S. Statistical mechanics of cellular automata // Rev. Modern Phys. – 1983. – 55(3). - P. 601–644.
46. Wolfram S. Cellular Automata as Models of Complexity // Nature. – 1984. – 311. - P. 419–424.
47. Wolfram S. Universality and complexity in cellular automata // Physica D. – 1984. – 10. - P. 1–35.
48. Wolfram S. Computation theory of cellular automata // Commun. Math. Phys. – 1984. – 96. - P. 15–57.
49. Wolfram S. Cryptography with Cellular Automata // Advances in Cryptology: Crypto '85 Proceedings. – Lecture Notes in Computer Science, vol. 218. – Springer-Verlag, 1986. - P. 429–432.
50. Wolfram S. Theory and applications of cellular automata: Including selected papers 1983-1986. – River Edge, NJ.: World Scientific Publishing Co., Inc., 1986.
51. Wolfram S. Cellular Automata and Complexity. – Addison-Wesley, Reading, 1994.
52. Wolfram S. A new kind of science. – Champaign, Ilinois: Wolfram Media Inc., 2002. – 1280 p.
53. Chopard B., Droz M. Cellular automata modeling of physical systems. – Cambridge: Cambridge University Press, 1998.
54. Deutch A., Dormann S. Cellular automaton modeling of biological pattern formation. – Birkhauser Boston Inc., 2004.
55. Gaylord R., Nishidate K. Modeling Nature – Cellular automata simulations with mathematica. – New York: Springer-Verlag, 1996.
56. Gaylord R., D'Andra L. Simulating society: A mathematica toolkit for modelling socioeconomic behavior. – New York: Springer-Verlag, 1998.
57. Gilbert N., Troitzsch K.G. Simulation for the Social Scientist. – Open University Press, 1999.
58. Goles E., Martinez S. (eds.) Cellular Automata and Complex Systems. – Kluwer, 1999.
59. Hoekstra A.G., Kroc J., Sloot P.M.A. (eds.) Simulating complex systems by cellular automata. – Springer, 2010. – 391 p.
60. Krugman P. The self-organizing economy. – New York: Blackman, 1996.
61. O'Sullivan D. Graph-based cellular automaton models of urban spatial processes // Ph.D. thesis. – University of London, London, United Kingdom. – 2000.
62. Schelling T.C., Dynamic models of segregation // J. of Math. Sociology. – 1971. – 1. - P. 143-186.
63. Vichniac G. Simulating physics with cellular automata // Physica D: Nonlinear Phenomena. – 1984. – 10. - P. 96–115.
64. Беркович С.Я. Клеточные автоматы как модель реальности: пер. с англ. – М.: Изд-во МГУ, 1993. – 112 с.
65. Евсютин О.О., Россошек С.К. Использование клеточных автоматов для решения задач преобразования информации // Доклады ТУСУРа. – 2010. – № 1 (21), часть 1. – С. 173–174.
66. Зотов Я.А. Использование клеточных автоматов в симметричной криптосистеме // Вопросы кибербезопасности. 2015. № 3 (11). С. 43-45.
67. Ключарёв П.Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. 2017. № 1 (19). С. 45-50.

CELLULAR AUTOMATA IN CRYPTOGRAPHY. Part 1

***A. Zhukov*[2]**

Cellular automata, known for more than 70 years, are one of the oldest computational models. Emerged in the late 40–ies of the XX century, the theory of cellular automata has given many theoretical and practical applications in the form of computational models for various natural facts and phenomena. Cellular automata are widespread and ubiquitous. They are independent objects of theoretical study, as well as a modeling tool in science and technology. The popularity of cellular automata is based on their relative simplicity combined with numerous possibilities for modeling sets of interconnected homogeneous objects. Besides that, cellular automata, as parallel structures, are perfectly useful for modeling discrete parallel processes, for creating parallel algorithms for information processing and are also a basis of computer technology with a highly parallel architecture.

***Keywords**: cellular automata models, set of finite automata, regular lattice, von Neumann neighborhood, algebraic solvability, cryptosystem, history of finite automata*

References

1. Toffoli T., Margolus N. Cellular automata machines: A new environment for modeling. – Cambridge, Mass.: MIT Press, 1987.
2. Sarkar P. A brief history of cellular automata, ACM Computing Surveys. – 2000. – Vol. 32, No. 1. - P. 80–107.
3. Sutner K. Classification of cellular automata, Encyclopedia of Complexity and Systems Science. – Springer, 2009.
4. Burks A.W. Essays on cellular automata. – Urban, IL: University of Illinois Press, 1970.
5. Mainzer K. Thinking in complexity. The computational dynamics of matter, mind, and mankind. – Berlin: Springer, 2007.
6. Mainzer K., Chua L. The Universe as automaton. – Springer, 2012. – 112 p.
7. Von Neumann, J. Theory of self-reproducing automata (edited and completed by A.W. Burks). – Urbana, IL: University of Illinois Press, 1966. – 388 p.
8. Schiff J.L. Cellular automata. A Discrete View of the World. – A John Wiley & Sons Inc., Publication. University of Auckland. – 2008.– 279 p.
9. Ulam S. On some mathematical problems connected with patterns of growth of figures, Proceedings of Symposia in Applied Mathematics. – 1962. – 14. - P. 215–224.

2 Aleksei Zhukov, Ph.D. (Math.), Associate Professor, Director at Association RusCrypto (Russian Branch of International Association of Cryptological Research), Moscow. E-mail: aez_iu8@rambler.ru

10. Wiener N., Rosenbluth A. The mathematical formulation of the problem of conduction of impulses in a network of connected excitable elements, specifically in cardiac muscle, Arch. Inst. Cardiol. Mex. – 1946. – 16. - P. 205–265.
11. Zuse K. Rechnender Raum. – Braunschweig: Friedrich Vieweg & Sohn, 1969. [Angl. perevod: Zuse K. Calculating Space. – Cambridge, Mass.: MIT Technical Translation, 1970.]
12. Berthold O. Computational universes. – Berlin: Humboldt Universitat zu Berlin, Institut fur Informatik, 2009. – 22 p.
13. Flake G.W. The computational beauty of Nature. – MIT Press, 1998.
14. Gernert D. Cellular automata and the concept of space, Becker J., Eisele I., Mündemann, F. (eds.) Parallelism, Learning, Evolution: Proceedings of the Workshop on Evolutionary Models and Strategies/Proceedings of the Workshop on Parallel Processing: Logic, Organization, and Technology (WOPPLOT 89). – LNAI vol. 565. – Springer-Verlag, 1989. - P. 94–102.
15. Ilachinski A. Cellular automata: A discrete Universe (2nd ed.) – World Scientific Publ. Co., 2002.
16. Kauffman S.A. At home in the Universe: The search for laws of self-organization and complexity. – Oxford: Oxford University Press, 1995.
17. Petrov P. Church-Turing thesis as an immature form of Zuse-Fredkin thesis, 3rd WSEAS International Conference on Systems Theory and Scientific Computation. Special session on cellular automata and applications. – 2003. URL: http://digitalphysics.org/Publications/Petrov/Pet02a2/Pet02a2.htm
18. Chaudhuri P.P., Chowdhury D.R., Nandi S., Chattopadhyay S. Additive cellular automata, theory and applications, vol. 1. – John Wiley & Sons, 1997.
19. Codd E.F. Cellular automata, ACM Monograph series. – New York & London: Academic Press, Inc., 1968.
20. Delorme M., Mazoyer J. Cellular automata: A parallel model, Mathematics and Its Applications, vol. 460. – Kluwer Academic Publishers, 1999.
21. Ganguly N., Sikdar B.K., Deutsch A., Canright G., Chaudhuri P.P. A survey on cellular automata. – 2004. URL: http://www.cs.unibo.it/bison/publications/CAsurvey.pdf
22. Griffeath D., Moore C. New Constructions in Cellular Automata. – Oxford University Press, 2003.
23. Kari J. Theory of cellular automata: a survey, Theoretical Computer Science. – 2005. – 334. - P. 3–33.
24. Kari J. Cellular automata. Lecture notes. – University of Turku, Finland, 2016. URL: http://users.utu.fi/jkari/ca2016/
25. Preston Jr. K., Duff M.J.B. Modern cellular automata: Theory and applications. – Plenum Press, 1984.
26. Rozenberg, G., Baeck, T., Kok, J. (eds.) Handbook of Natural Computing. – Berlin: Springer, 2011.
27. Schiff J.L. Introduction to cellular automata. URL: http://psoup.math.wisc.edu/pub/Schiff_CAbook.pdf
28. Toffoli T., Margolus N. Invertible cellular automata: a review, Physica D. – 1990. – 45, 1-3. - P. 229–253.
29. Vivien H. An introduction to cellular automata. – 2003. URL: https://www.irif.fr/~yunes/ca/archives/bookvivien.pdf
30. Kudryavtsev V.B., Podkolzin A.S., Bolotov A.A. Osnovy teorii odnorodnykh struktur. – M.: Nauka, 1990.
31. Banks E.R. Information and Transmission in Cellular Automata, Ph.D. diss. – Massachusetts Institute of Technology, 1971.
32. Moore E.F. Machine models of self-reproduction, Proceedings of Symposia in Applied Mathematics. – 1962. – 14. - P. 17–33.
33. Langton C. Self-reproduction in cellular automata, Physica D. – 1984. –10. - P. 135–144.
34. Sipper M. Fifty years of research on self-replication: An overview, Artificial Life. – 1998. – 4. - P. 237–257.
35. Hedlund G. Endomorphisms and automorphisms of shift dynamical systems, Math. Systems Theory. – 1969. – 3. - P. 320–375.
36. Gardner M. Mathematical games: The fantastic combinations of John Conway›s new solitaire game «Life», Scientific American. – 1970. – 223. - P. 120–123.
37. Gardner M. On cellular automata, self-reproduction, the Garden of Eden and the game of «Life, Scientific American. – 1971. – 224. - P. 112–117.
38. Gardner M. Matematicheskie dosugi. – M.: Mir, 1972.
39. Mitchell M. Computation in cellular automata: A selected review, Gramss T., Bornholt S., Gross M., Mitchell M., Pellizzari T. (eds.) NonStandard Computation. – Weinheim: Wiley-VCH, 1998. - P. 95–140.
40. Morita K., Harao M. Computation Universality of one dimensional reversible injective cellular automata, IEICE Trans. – 1989. – E 72. - P. 758–762.
41. Ollinger N. Universalities in cellular automata; a (short) survey, Durand B. (ed.) Proceedings JAC 2008. – 2008. - P. 102–118.
42. Toffoli T. Computation and construction universality of reversible cellular automata, Journal of Computer and System Sciences. – 1977. – 15, N2. - P. 213–231.
43. Smith III A. Cellular automata complexity trade-offs, Inf. Control. – 1971. – 18. - P. 466–482.
44. Smith III A. Introduction to and survey of polyautomata theory, Automata, Languages, Development. – Amsterdam: North-Holland Publishing Co., 1976.
45. Wolfram S. Statistical mechanics of cellular automata, Rev. Modern Phys. – 1983. – 55(3). - P. 601–644.
46. Wolfram S. Cellular Automata as Models of Complexity, Nature. – 1984. – 311. - P. 419–424.
47. Wolfram S. Universality and complexity in cellular automata, Physica D. – 1984. – 10. - P. 1–35.
48. Wolfram S. Computation theory of cellular automata, Commun. Math. Phys. – 1984. – 96. - P. 15–57.
49. Wolfram S. Cryptography with Cellular Automata, Advances in Cryptology: Crypto '85 Proceedings. – Lecture Notes in Computer Science, vol. 218. – Springer-Verlag, 1986. - P. 429–432.
50. Wolfram S. Theory and applications of cellular automata: Including selected papers 1983-1986. – River Edge, NJ.: World Scientific Publishing Co., Inc., 1986.
51. Wolfram S. Cellular Automata and Complexity. – Addison-Wesley, Reading, 1994.
52. Wolfram S. A new kind of science. – Champaign, Ilinois: Wolfram Media Inc., 2002. – 1280 p.
53. Chopard B., Droz M. Cellular automata modeling of physical systems. – Cambridge: Cambridge University Press, 1998.
54. Deutch A., Dormann S. Cellular automaton modeling of biological pattern formation. – Birkhauser Boston Inc., 2004.
55. Gaylord R., Nishidate K. Modeling Nature – Cellular automata simulations with mathematica. – New York: Springer-Verlag, 1996.
56. Gaylord R., D'Andra L. Simulating society: A mathematica toolkit for modelling socioeconomic behavior. – New York: Springer-Verlag, 1998.
57. Gilbert N., Troitzsch K.G. Simulation for the Social Scientist. – Open University Press, 1999.
58. Goles E., Martinez S. (eds.) Cellular Automata and Complex Systems. – Kluwer, 1999.
59. Hoekstra A.G., Kroc J., Sloot P.M.A. (eds.) Simulating complex systems by cellular automata. – Springer, 2010. – 391 p.
60. Krugman P. The self-organizing economy. – New York: Blackman, 1996.
61. O'Sullivan D. Graph-based cellular automaton models of urban spatial processes, Ph.D. thesis. – University of London, London, United Kingdom. – 2000.
62. Schelling T.C., Dynamic models of segregation, J. of Math. Sociology. – 1971. – 1. - P. 143-186.
63. Vichniac G. Simulating physics with cellular automata, Physica D: Nonlinear Phenomena. – 1984. – 10. - P. 96–115.
64. Berkovich S.Ya. Kletochnye avtomaty kak model› real›nosti: per. s angl. – M.: Izd-vo MGU, 1993. – 112 p.
65. Evsyutin O.O., Rossoshek S.K. Ispol›zovanie kletochnykh avtomatov dlya resheniya zadach preobrazovaniya informatsii, Doklady TUSURa. – 2010. – N 1 (21), Part.1 – P. 173–174.
66. Zotov Ya.A. Ispol›zovanie kletochnykh avtomatov v simmetrichnoy kriptosisteme, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. N 3 (11). S. 43-45.
67. Klyucharev P.G. Metod postroeniya kriptograficheskikh khesh-funktsiy na osnove iteratsiy obobshchennogo kletochnogo avtomata, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. N 1 (19). P. 45-50.