КЛЕТОЧНЫЕ АВТОМАТЫ И ИХ ОБОБЩЕНИЯ В ЗАДАЧАХ КРИПТОГРАФИИ. ЧАСТЬ 1

Ключарёв П.Г.[1]

Цель статьи: *аналитический обзор применения клеточных автоматов и их обобщений в криптографии.*
Метод исследования: *анализ научных публикаций по теме статьи.*
Полученные результаты: *в обзорной статье проанализирована литература, посвященная использованию как классических клеточных автоматов, так и их обобщений для построения криптографических алгоритмов. Статья состоит из двух частей. Первая часть посвящена классическим клеточным автоматам и основанным на них симметричным криптографическим алгоритмам. В ней кратко обсуждается история теории клеточных автоматов и ее применения в различных научных областях. Приведен обзор работ ряда авторов, которыми предлагались симметричные криптографические алгоритмы и генераторы псевдослучайных последовательностей, основанные на одномерных клеточных автоматах. Стойкость таких криптоалгоритмов оказалось недостаточной. Далее дан обзор статей, посвященных использованию двухмерных клеточных автоматов для построения симметричных криптоалгоритмов (этот подход давал лучшие результаты). Также упомянуты многомерные клеточные автоматы. Вторая часть .статьи, которая будет опубликована, в следующем номере, будет посвящена обзору работ, посвященных использованию обобщенных клеточных автоматов в криптографии – на основе таких автоматов возможно создавать алгоритмы симметричного шифрования и криптографические хэш-функции, обладающие высоким уровнем криптостойкости и высокой производительностью при аппаратной реализации (например, на программируемых логических интегральных схемах), а также предъявляющие достаточно низкие требования к аппаратным ресурсам. Кроме того, в ней будет уделено внимание интересным связям обобщенных клеточных автоматов, в контексте их использования в криптографии, с теорией расширяющих графов; также будет уделено внимание вопросам стойкости криптоалгоритмов, основанных на обобщенных клеточных автоматах. Будут упомянуты работы, посвященные реализации различных криптографических алгоритмов, основанных на обобщенных клеточных автоматах, на программируемых логических интегральных схемах и графических процессорах. Кроме того, будет дан обзор асимметричных криптоалгоритмов, основанных на клеточных автоматах. Будут рассмотрены вопросы о принадлежности некоторых задач на клеточных автоматах и их обобщениях к классу NP-полных задач, а также к некоторым другим классам сложности.*

Ключевые слова: *криптографические алгоритмы, стойкость криптоалгоритмов, поточный шифр, блочный шифр, хэш-функция.*

DOI:10.21681/2311-3456-2021-6-90-101

Введение

Бурное развитие информационных технологий привело к резкому повышению требований к защите информации. Одними из основных методов защиты информации являются криптографические методы. Современная криптография развивается весьма активно и становится все более и более востребованной. При этом предъявляются высокие требования не только к стойкости современных криптографических алгоритмов, но и к их быстродействию. Это связано с тем, что пропускная способность каналов связи быстро возрастает, например, в 2017 г. принят стандарт IEEE 802.3bs-2017 на протоколы организации компьютерных сетей, функционирующие на скоростях 200 и 400 Гбит/с, а в 2020 г. принят стандарт IEEE 802.3ck-2020 на протоколы, позволяющие достичь скорости 800 Гбит/с. В то же время все более часто используются вычислительные устройства с малыми вычислительными ресурсами. Такие устройства применяются в широчайшей гамме областей, начиная от многочисленных применений в гражданской сфере, например в интернете вещей, в котором передаваемая информация должна быть должным образом защищена, и заканчивая различными системами вооружений (в рамках концепции сетецентрической войны), компоненты которых должны эффективно взаимодействовать между собой с помощью обмена информацией, обеспечивая при этом надежность и конфиденциальность, причем в условиях активного использования противником разнообразных средств противодействия. Все это обуславливает необходимость разработки новых симметричных криптографических алгоритмов, таких как блочные шифры, поточные шифры и криптографические хэш-функции.

В области асимметричной криптографии (криптографии с открытым ключом) выделяется направление постквантовой криптографии, занимающееся асимметричными криптографическими алгоритмами, для взлома которых не существует эффективных квантовых алгоритмов.

1 Ключарёв Петр Георгиевич, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: pk.iu8@yandex.ru

Клеточные автоматы — модель, которая нашла применения в разных областях как чистой математики, так и ее приложений. Теория алгоритмов, теория хаоса, теоретическая физика, биология, эпидемиология, химия, экология, вирусология, социология — далеко не полный список научных дисциплин, в которых клеточные автоматы находят то или иное применение. Попытки применить клеточные автоматы в криптографии начались в середине 1980-х гг., причем их применение выглядело весьма многообещающим. С одной стороны, ряд их теоретических свойств позволял надеяться на то, что они позволят обеспечить высокий уровень криптостойкости, с другой стороны, присущий им параллелизм обработки информации давал основания ожидать высокой скорости работы основанных на них алгоритмов, в особенности, при аппаратной реализации. К сожалению, первые эксперименты в этой области оказались не очень удачными, что привело к определенному снижению интереса к криптографическому использованию этих моделей. В 2009 – 2011 гг. вышла серия работ, которая вновь подогрела интерес к этому направлению: оказалось, что с помощью двухмерных клеточных автоматов и обобщенных клеточных автоматов можно построить поточные шифры, обладающие высокой производительностью при аппаратной реализации и в то же время довольно низкими требованиями к аппаратным ресурсам. В дальнейшем вышло большое число работ, подводящих теоретический базис под использование обобщенных клеточных автоматов в симметричной криптографии и предлагающих новые криптоалгоритмы на основе таких автоматов. Кроме того, известны подходы к построению асимметричных криптоалгоритмов на основе клеточных автоматов. Есть определенная надежда, что такие подходы в будущем позволят получить новые асимметричные криптоалгоритмы, в том числе, постквантовые.

Данный обзор посвящен использованию клеточных автоматов (в том числе, обобщенных) в криптографии.

1. Клеточные автоматы

Неформально говоря, клеточный автомат — это автономный автомат, состояние которого задано упорядоченным набором ячеек памяти, образующих k-мерную решетку. В каждой ячейке такого автомата может храниться одно значение, принадлежащее некоторому конечному множеству (в большинстве случаев, в литературе рассматриваются двоичные клеточные автоматы, у которых этим множеством является $\mathbb{Z}_2$).

Автомат работает по шагам (тактам). Значения всех ячеек изменяются одновременно на каждом шаге, в соответствии с некоторыми правилами перехода. При этом значение ячейки памяти на очередном шаге зависит только от значений ячеек, принадлежащих некоторой ее окрестности, на предыдущем шаге, а правила перехода являются одинаковыми для всех ячеек решетки клеточного автомата. В теоретических работах могут рассматриваться клеточные автоматы с бесконечной решеткой. В случае конечной решетки обычно для того, чтобы правила перехода можно было сделать одинаковыми для каждой ячейки, противоположные края решетки отождествляются (т.е. решетка превращается в тор). Набор значений ячеек на данном шаге называется заполнением клеточного автомата. Заполнение в начальный момент времени называется начальным заполнением.

Более формальные определения будут даны ниже – отдельно для одномерного клеточного автомата и для двухмерного клеточного автомата, а также, в соответствующем разделе второй части, будет дано определение обобщенного клеточного автомата.

Понятие клеточного автомата было предложено Джоном фон Нейманом в работе [1]. Фон Нейман использовал клеточные автоматы в качестве модели самоорганизующихся систем. На его исследования существенно повлиял Станислав Улам[2], который пришел к подобным моделям, занимаясь математическим моделированием роста кристаллов. Затем такие автоматы широко исследовались различными авторами. Клеточным автоматам посвящено большое количество монографий (в частности, [2–11]) и статей (следует, в частности, упомянуть работы [12–14]). Особенно много клеточными автоматами занимался Стивен Вольфрам, который подробно исследовал различные их свойства, в том числе и те, которые относятся к криптографии и генерации случайных последовательностей. Основные результаты С. Вольфрама опубликованы в работах [11,12,14–16], а также многих других. Целый ряд его работ, посвященных клеточным автоматам, опубликован в книге [17].

Описанию истории развития теории клеточных автоматов посвящен обзор [18], а также книга [19]. Отметим также обзор [20].

Существует следующая классификация клеточных автоматов, предложенная С. Вольфрамом в книге [11]:

- Класс 1: Поведение автомата является очень простым. Почти все начальные заполнения быстро приводят к одному и тому же финальному состоянию.
- Класс 2: Существует большое количество возможных финальных состояний, но все они состоят из некоторого множества простых структур, которые либо остаются стабильными, либо повторяются с маленьким периодом. Локальные изменения в начальных условиях оказывают влияние локального характера на дальнейшую динамику автомата.
- Класс 3: Результатом эволюции почти всех начальных заполнений являются псевдослучайные последовательности. Стабильных структур не возникает. Локальные изменения в начальном

2 Станислав Улам, родился в 1909 г. в зажиточной еврейской семье, окончил Львовский политехнический институт (в то время Польша), получив в 1933 г степень доктора философии. В 1935 г. он познакомился в Варшаве с фон Нейманом, который пригласил его в Принстон, куда он переехал в 1936 г., что его и спасло, так как оставшиеся во Львове отец и сестра (мать, родом из Стрыя, умерла в 1938 г.) погибли в гетто между 1941 и 1943 гг. Участвовал в создании водородной бомбы в Лос-Аламосской лаборатории. Выдвинул теорию ядерного ракетного двигателя, предложил вычислительный метод Монте-Карло, сформулировал вместе с Ферми и другими учеными парадокс в теории хаоса, сейчас называемый парадокс Ферми-Паста-Улама-Цинга. До конца жизни в мае 1984 г. жил и работал в США (прим. редакции).

заполнении оказывают сильное влияние на ход всей эволюции системы.

- Класс 4: Результатом эволюции почти всех начальных заполнений являются структуры, которые взаимодействуют сложным образом с формированием локальных устойчивых структур. Локальные изменения в начальном заполнении оказывают сильное влияние на ход всей эволюции системы. Некоторые клеточные автоматы этого класса являются полными по Тьюрингу.

Большая часть исследователей занимались клеточными автоматами класса 2 и класса 4, т.к. они демонстрируют много интересных свойств с точки зрения теории динамических систем, теории алгоритмов и др. В то же время с криптографической точки зрения, наиболее интересны клеточные автоматы из класса 3.

2. Клеточные автоматы в науке и технике

Клеточные автоматы весьма широко применяются в различных разделах науки и техники, напрямую не связанных с криптографией. Здесь мы приведем некоторые сведения о таких применениях, несмотря на то что настоящий обзор посвящен прежде всего использованию клеточных автоматов в криптографии. Учитывая, что приложениям клеточных автоматов посвящены десятки тысяч статей, написанных специалистами в самых разных областях знаний, полный обзор этих приложений вряд ли возможен. Поэтому в этом разделе мы лишь обозначим основные направления и приведем ссылки на некоторые обзорные статьи и книги.

Клеточные автоматы активно изучаются в различных областях математики и теоретической информатики, имеется огромное число публикаций. Интерес к клеточным автоматам объясняется, в частности тем, что они представляют собой как простую математическую модель, которая хорошо подходит для описания динамики разнообразных систем, так и весьма любопытную вычислительную модель параллельной обработки информации. Теорией клеточных автоматов, с точки зрения теории конечных автоматов, математической логики и смежных областей, много занималась и занимается научная школа В.Б. Кудрявцева. Среди большого числа работ, принадлежащих членам этой научной школы, отметим обзоры [21,22] и ставшую классической монографию [23]. Теорией клеточных автоматов, с точки зрения теории вычислимости и теории динамических систем, занимался С. Вольфрам, которому принадлежит целый ряд основополагающих работ в этой области (сошлемся здесь на сборник его статей по клеточным автоматам [24]). Также клеточные автоматы находят применение в области вычислительной геометрии и обработки изображений [10].

Теория динамических систем очень богата на применения клеточных автоматов [25]. Причем как с точки зрения теории, так и с точки зрения приложений в задачах имитационного моделирования в различных областях. Многие биологические системы естественным образом моделируются с помощью клеточных автоматов. Обзор этого направления можно найти, например, в книге [26]. В частности, клеточные автоматы применяют для моделирования пролиферации и взаимодействия живых клеток, роста опухолей, динамики популяций организмов, развития эпидемий [27] и др. В области химии клеточные автоматы применяются для математического моделирования процессов диффузии жидкостей и газов, процессов кристаллизации, процессов адсорбции, процессов коррозии. Целый ряд химических реакций может быть описан в терминах клеточных автоматов. Хороший обзор этого направления представлен в работе [28], а также в монографии [29]. Также клеточные автоматы применяются в задачах анализа микроструктуры металлов [30]. В геоинформационных системах и связанных с ними задачах имитационного моделирования городов также активно применяются клеточные автоматы: [31–33]. Вообще, клеточные автоматы активно применяются в задачах имитационного моделирования сложных систем, в том числе, социальных и экономических [34].

Интереснейшие приложения клеточные автоматы нашли в теоретической физике, в рамках так называемой цифровой физики — совокупности теоретических взглядов, основанных на подходе к описанию Вселенной, как к результату работы некоторого вычислительного устройства. Родоначальником этой области являлся Конрад Цузе, который в книге [35] высказал мысль, что таким вычислительным устройством может являться клеточный автомат. Развитием клеточно-автоматного описания Вселенной занимался уже многократно упомянутый С. Вольфрам — этому он уделяет внимание в книге [11], а его недавняя книга [36] посвящена этому полностью.

Изучению клеточных автоматов и их приложений традиционно уделяется большое внимание в нашей стране. Российским публикациям в этой области посвящен отличающийся полнотой обзор [37].

Популяризации клеточных автоматов весьма содействовала игра «Жизнь», придуманная Джоном Конвеем в конце 1960х гг. и популяризованная Мартином Гарднером, который опубликовал статью о ней в научно-популярном журнале Scientific American [38]. Научным подробностям этой игры посвящена книга [3].

Таким образом, клеточные автоматы активно исследуются и находят многочисленные применения в самых разных областях науки и техники. Ежегодно публикуется большое количество работ, проводится несколько крупных международных научных конференций, посвященных клеточным автоматам.

3. Одномерные клеточные автоматы в симметричной криптографии

3.1. Основные понятия

С. Вольфрамом было, прежде всего, исследовано применение в криптографии одномерных клеточных автоматов. Одномерный клеточный автомат — это автономный автомат, состояние которого задается набором ячеек памяти m_i. В теоретических работах достаточно часто рассматривают бесконечные одномерные клеточные автоматы, в которых набор ячеек представляет собой что-то вроде бесконечной в обе стороны ленты:

$(\ldots, m_{-1}, m_0, m_1, \ldots)$. Работает такой автомат по шагам. Обозначим значение ячейки m_i на шаге t через $m_i(t)$. На каждом такте работы автомата значения всех ячеек одновременно изменяются в зависимости от значений соседних ячеек:

$$m_i(t+1) = f(m_{i-a}(t), \ldots, m_{i+b}(t)), \quad (1)$$

где функция f называется локальной функцией связи.

На практике количество ячеек ограничивают некоторым N: $(m_0, m_2 \ldots, m_{N-1})$ и набор ячеек зацикливают так, что эволюция клеточного автомата вместо уравнения (1) описывается уравнением:

$$m_i(t+1) = f(m_{(i-a) \mod N}(t), \ldots, m_{(i+b) \mod N}(t)), \quad (2)$$
$$i \in \mathbb{Z}_N, t = 0,1,\ldots$$

При этом, клеточный автомат может быть определен над тем или иным множеством. Чаще всего рассматривается двоичный случай, когда $m_i(t) \in \mathbb{Z}_2$. В этом случае локальная функция связи является булевой.

Выделяют класс элементарных клеточных автоматов, у которых в формулах (1) и (2) полагают $a = b = 1$. Всего существует 256 элементарных клеточных автоматов. Для них вводят нумерацию (так называемые коды Вольфрама), рассматривая вектор значений локальной функции связи как число, следующим образом:

$$n_{CA} = 2^7 f(1,1,1) + 2^6 f(1,1,0) + 2^5 f(1,0,1) + 2^4 f(1,0,0) +$$
$$+2^3 f(0,1,1) + 2^2 f(0,1,0) + 2 f(0,0,1) + f(0,0,0). \quad (3)$$

Обычно элементарный клеточный автомат с номером n_{CA} называют rule n_{CA}.

3.2 Поточные шифры и генераторы псевдослучайных последовательностей на основе одномерных клеточных автоматов

Стивен Вольфрам впервые предложил использовать клеточные автоматы для генерации криптографически стойких псевдослучайных последовательностей и поточного шифрования в работах [14,16]. В них используется клеточный автомат rule 30, работа которого описывается уравнением:

$$m_i(t+1) = m_{i-1}(t) \oplus m_i(t) \oplus m_{i+1}(t) \oplus m_i(t) m_{i+1}(t),$$

$$(t), \quad i \in \mathbb{Z}_N, t = 0,1,\ldots$$

В начальный момент времени (при $t = 0$) ячейки инициализируются начальными значениями (вырабатываемыми на основе ключа). Выходной последовательностью такого генератора является последовательность значений некоторой ячейки клеточного автомата (с некоторым фиксированным индексом s):

$$\gamma_t = m_s(t), \quad t = 1,2,\ldots$$

Такой генератор вырабатывает один двоичный разряд за один такт. Согласно результатам С. Вольфрама, выходная последовательность такого генератора имеет хорошие статистические свойства. Клеточный автомат rule 30 реализует функцию достаточно близкую к биекции (лишь около 0.85^N из 2^N вершин графа состояний имеют больше одного предка, см. рис. 1). Также, по полученным С. Вольфрамом результатам, при достаточно большом N, подавляющее большинство состояний автомата лежат на одном большом цикле, длина которого приблизительно равна $2^{0,61 \cdot N}$.

К сожалению, в результате проведенного в работе [39] криптоанализа, предложенный С. Вольфрамом шифр оказался нестойким.

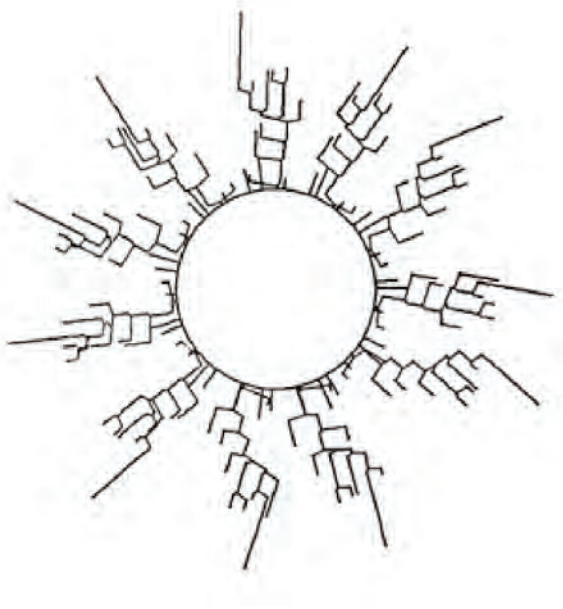

Рис. 1. Граф переходов одномерного элементарного клеточного автомата Rule 30 с 11 ячейками (иллюстрация из статьи [14]).

На основе одномерных клеточных автоматов предлагались и более сложные шифры. Так, в работе [40] предлагался поточный шифр, в котором, в сочетании с довольно простыми нелинейными преобразованиями, использовался одномерный клеточный автомат с линейной локальной функцией связи, но в работе [41] этот шифр был взломан. В работе [42] был предложен шифр, использующий ту же схему, что и известный поточный шифр Trivium [43], однако вместо нелинейных регистров сдвига с обратными связями, в нем использовались одномерные клеточные автоматы. В работе [44] был предложен еще один поточный шифр, в котором используется своеобразный «сэндвич» из одномерных клеточных автоматов с линейными и нелинейными локальными функциями связи, часть из которых генерируется динамически. К сожалению, криптостойкость этих шифров не была удовлетворительно исследована.

Криптографические свойства одномерных клеточных автоматов изучались в ряде работ. В частности, в работах [45,46] изучается связь линейных одномерных клеточных автоматов с линейными регистрами сдвига с обратной связью и структурами на них основанными. В работе [47] выбираются одномерные клеточные автоматы с хорошими статистическими свойствами выходной последовательности, а в работе [48] для решения этой задачи применяются генетические алгоритмы.

Несмотря на то, что с помощью одномерных клеточных автоматов возможно получить достаточно хорошие статистические свойства выходной последовательно-

сти, основанные на них криптографические алгоритмы имеют ряд проблем с криптостойкостью и невысокую производительность. Криптостойкость ряда предлагавшихся поточных шифров, основанных на одномерных клеточных автоматах, не была удовлетворительно исследована, а те из них, чья криптостойкость была исследована, оказались нестойкими. Подобные криптоалгоритмы критикуются, например в работах [39,49,50] и др. В связи с этими недостатками, алгоритмы, основанные на одномерных клеточных автоматах, редко используются для генерации псевдослучайных последовательностей на практике. Один из позитивных примеров практического применения подобных алгоритмов – в системе компьютерной алгебры Wolfram Mathematica [51], где одномерный клеточный автомат применяется для генерации не являющихся криптографически стойкими псевдослучайных последовательностей.

3.3 Блочные шифры на основе одномерных клеточных автоматов

Рядом авторов были построены блочные шифры, основанные на одномерных клеточных автоматах. В работе [52] предложен блочный шифр, один раунд которого представляет собой смешивание с раундовым ключом (путем поразрядного сложения по модулю 2 с ним), за которым следует применение трех преобразований: нелинейного, линейного и обратного к нелинейному. Нелинейное преобразование состоит из определенного числа шагов элементарного клеточного автомата rule 30, а линейное преобразование состоит из определенного числа шагов элементарного клеточного автомата rule 153. К сожалению, криптостойкость данного шифра не исследовалась.

В работе [53] предложен блочный шифр, основанный на схеме Фейстеля, в качестве раундовой функции которой используется одномерный клеточный автомат rule 30. На этот автомат подается поразрядная сумма подблока и раундового ключа. Между раундами применяются обратимый S-блок и P-блок. В работе [53] проведено исследование статистических свойств данного шифра, однако убедительных обоснований преимуществ такого шифра не приведено, как не приведено и удовлетворительного исследования его криптостойкости.

Из общих соображений представляется интересной концепция использования обратимых клеточных автоматов для построения блочных шифров. Действительно, это может позволить получить высокое быстродействие таких шифров. К сожалению, теория синтеза обратимых клеточных автоматов все еще недостаточно развита. Например, в статье [54] предлагается использовать обратимый одномерный клеточный автомат из некоторого семейства. Причем конкретный автомат выбирается на основе ключа. В статье заключается, что использование одного автомата не позволяет добиться высокой криптостойкости. Тем не менее, этот подход развит в статье [55], в которой используется несколько одномерных клеточных автоматов, а ключ подмешивается с помощью поразрядного сложения по модулю 2. Достаточного обоснования криптостойкости такого подхода не приводится.

К сожалению, для большинства известных блочных шифров, основанных на клеточных автоматах, не проводилось независимых попыток криптоанализа. Исключением является предложенный в работе [56] блочный шифр, основанный на одномерном клеточном автомате над полем $\mathbb{F}_{2^8}$, состоящим из 16 ячеек. Таких автоматов в нем используется два. Один из них применяется для генерации второго клеточного автомата и других параметров, исходя из ключа, а с помощью второго – происходит шифрование очередного блока (кроме второго автомата в шифровании участвуют другие преобразования, зависящие от сгенерированных параметров). Шифр обладает достаточно сложной и остроумной структурой, однако, согласно работе [57], в нем, к сожалению, были найдены уязвимости.

3.4 Криптографические хэш-функции на основе одномерных клеточных автоматов

Пожалуй, впервые криптографическая хэш-функция на основе клеточного автомата была предложена И. Дамгордом в работе [58]. Основной принцип работы этой хэш-функции заключался в использовании одномерного элементарного клеточного автомата rule 30. Причем выполняется 384 шага этого клеточного автомата. Способ построения коллизий к этой хэш-функции был предложен в работе Й. Даймена [59]. В ней же предложена другая хэш-функция, отличающаяся тем, что используется более сложная локальная функция связи, такая что каждая ячейка зависит от девяти ячеек на предыдущем шаге.

Далее рядом авторов был предложен целый ряд разнообразных криптографических хэш-функций на базе клеточных автоматов. В частности, хэш-функции, основанные на одномерных клеточных автоматах, предлагаются в работах [60–67]. К сожалению, использование одномерных клеточных автоматов не позволяет достичь высокой производительности, что продемонстрировано в статье [67], где производительность такой функции на ПЛИС не достигает даже 0.5 МБ/с.

Предложенные в упомянутых работах хэш-функции основаны либо на схеме Меркла-Дамгорда [58], либо на древовидной схеме, либо на схеме криптографической губки [68]. В случае схемы Меркла-Дамгорда, на которой основаны хэш-функции, предложенные в работах [62,63,65], и древовидной схемы, на которой основаны хэш-функции, предложенные в работах [60,61], однонаправленная функция сжатия построена на базе нескольких шагов одномерного клеточного автомата, в сочетании с некоторыми другими преобразованиями, такими как S-блоки, циклические сдвиги и др. В случае схемы криптографической губки, на которой основаны хэш-функции, предложенные в работах [64,66], в качестве функции преобразования также используется несколько шагов одномерного клеточного автомата.

К сожалению, криптостойкость большинства основанных на одномерных клеточных автоматах хэш-функций либо не изучена вообще, либо изучена недостаточно.

3.5 Перспективы одномерных клеточных автоматов в симметричной криптографии

Несмотря на то, что существовало достаточно много попыток применения одномерных клеточных

автоматов в симметричной криптографии, использующие их симметричные криптографические алгоритмы либо не анализировались вовсе, либо были взломаны. Симметричные криптоалгоритмы, основанные на одномерных клеточных автоматах, обычно предназначены для аппаратной реализации, однако вызывают вопросы с точки зрения производительности. Одним из недостатков одномерных клеточных автоматов, с точки зрения криптографии, является тот факт, что для того, чтобы обеспечить зависимость значений всех ячеек от начального значения каждой из них, требуется линейное относительно числа ячеек количество шагов. Из-за этого производительность основанных на них алгоритмов невысока.

Все это позволяет предположить, что одномерные клеточные автоматы вряд ли позволяют производить построение криптостойких и в то же время высокопроизводительных симметричных криптографических алгоритмов.

4. Двух- и более мерные клеточные автоматы в симметричной криптографии

4.1. Двух- и более мерные клеточные автоматы: основные понятия

Двухмерным клеточным автоматом будем называть автономный автомат, состояние которого задается набором ячеек памяти, расположенных в узлах целочисленной решетки на плоскости. Как уже говорилось, в теоретических работах могут рассматриваться клеточные автоматы с бесконечным числом ячеек. Для прикладных целей более интересны автоматы с конечным числом ячеек, образующих на плоскости прямоугольник. При этом, достаточно часто отождествляют противоположные края решетки, чтобы правила перехода можно было сделать одинаковыми для каждой ячейки. В начальный момент времени каждая ячейка $m_{i,j}$ имеет некоторое начальное значение $m_{i,j}(0)$. Автомат работает пошагово. Значение каждой ячейки на шаге t вычисляется как функция f, называемая локальной функцией связи, от значений ячеек, принадлежащих некоторой окрестности этой ячейки.

Обычно значения ячеек являются двоичными (хотя, как уже говорилось, могут рассматриваться и клеточные автоматы над другими множествами). Под окрестностью порядка s ячейки $m_{i,j}$ обычно понимается набор ячеек, находящихся от нее на расстоянии, не превышающим s. При этом, можно использовать разные метрики. Например, если использовать манхеттенское расстояние, то получится окрестность фон Неймана: $\{(u,v)\,|\,|u-i|+|v-j|\leqslant s\}$, а если использовать расстояние Чебышева, то получится окрестность Мура: $\{(u,v)\,|\,|u-i|\leqslant s,|v-j|\leqslant s\}$. Часто в окрестность не включают центральную ячейку (т.е. саму ячейку $m_{i,j}$), в этом случае, окрестность называется неполной.

Кроме двухмерных можно рассматривать и k-мерные клеточные автоматы при $k\geqslant 3$, заменив плоскость k-мерным пространством.

Симметричные криптографические алгоритмы, основанные на двух- и более мерных клеточных автоматах, потенциально позволяют достичь более высокой производительности, чем симметричные криптоалгоритмы на основе одномерных клеточных автоматов, т.к. в случае использования правильно выбранного k-мерного клеточного автомата с N ячейками, чтобы обеспечить зависимость значений всех ячеек от начального значения каждой из них, требуется порядка $O(\sqrt[k]{N})$ шагов.

4.2 Криптоалгоритмы на основе двухмерных клеточных автоматов

Долгое время заслуживающих упоминания криптографических алгоритмов, основанных на двухмерных клеточных автоматах, не предлагалось. Однако в 2009 – 2011 гг. вышла целая серия статей [69–78] и диссертация [79] Б.М. Сухинина, который смог весьма удачно применить двумерные клеточные автоматы для генерации псевдослучайных последовательностей. Им введено понятие интегральной и пространственной характеристик лавинного эффекта для клеточных автоматов и предложен генератор псевдослучайных последовательностей, основанный на клеточных автоматах.

Характеристики лавинного эффекта отражают влияние инверсии значения одной ячейки на дальнейшую эволюцию клеточного автомата. При этом рассматриваются два идентичных клеточных автомата, различающихся в начальный момент времени лишь значением одной ячейки. Интегральная характеристика лавинного эффекта клеточного автомата — это функция, отражающая зависимость от номера шага отношения числа ячеек, различающихся у этих двух клеточных автоматов, к числу ячеек клеточного автомата. Пространственная характеристика лавинного эффекта клеточного автомата — это функция, отражающая зависимость от номера шага отношения максимального расстояния, на котором имели место различия, к максимально возможному расстоянию между ячейками данного клеточного автомата. Важным является то, как быстро эти характеристики достигнут оптимальных значений: 1/2 для интегральной и 1 для пространственной характеристики.

Предложенная Б.М. Сухининым схема генератора псевдослучайных последовательностей состоит из двух клеточных автоматов и регистра сдвига. Схема такого генератора изображена на рис. 2. Оба клеточных автомата являются двухмерными, имеют размер 37×11 ячеек, при этом используется неполная окрестность Мура. Выход каждого автомата снимается с ячеек, образующих прямоугольник 32×8. При этом локальная функция связи является равновесной булевой функцией. Она, путем рандомизированного перебора, выбиралась так, чтобы выходная последовательность такого генератора успешно проходила статистические тесты из комплекта NIST Statistical Test Suite. Линейный регистр сдвига с обратной связью используется в этой схеме для обеспечения гарантированной длины периода выходной последовательности. Его выход на каждом шаге прибавляется по модулю 2 к значению одной из ячеек каждого клеточного автомата. Такой генератор можно рассматривать как генератор гаммы поточного шифра. Он имеет высокую производительность при аппаратной реализации (на ПЛИС): была достигнута производительность в 34 Гбит/с при требованиях к аппаратным ресурсам 21892 LE.

DOI:10.21681/2311-3456-2021-6-90-101

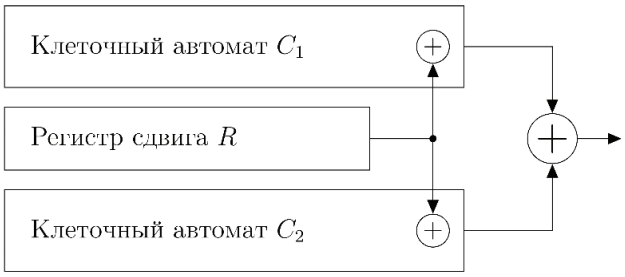

Рис. 2: Структура генератора псевдослучайных последовательностей, предложенная в работе [79]

Предлагались и другие криптоалгоритмы на основе двухмерных клеточных автоматов. В частности, в работах [80,81] построены криптографические хэш-функции, основанные на двухмерных клеточных автоматах. Они используют схему криптографической губки (Sponge), в качестве функции преобразования в них применяется определенное число шагов двухмерного клеточного автомата. Различаются они, по существу, локальной функцией связи. К сожалению, удовлетворительного исследования криптостойкости этих хэш-функций проведено не было.

Заключение

Клеточные автоматы являются весьма интересной алгоритмической моделью, которая может использоваться при построении симметричных криптографических алгоритмов. Особенно перспективными выглядят двухмерные клеточные автоматы. Весьма многообещающий подход, связанный с обобщенными клеточными автоматами будет рассмотрен во второй части статьи. Кроме того, во второй части будет уделено внимание некоторым теоретико-сложностным аспектам теории клеточных автоматов, а также будет дан обзор асимметричных криптоалгоритмов, основанных на клеточных автоматах.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-17-50258.

Литература

1. von Neumann J. The general and logical theory of automata // Proc. Hixon Symposium on Cerebral Mechanisms in Behavior / Ed. by L. A. Jeffress. New York, 1951. P. 1–31.
2. Тоффоли Т., Марголус Н. Машины клеточных автоматов. М.: Мир, 1991. 280 с.
3. Adamatzky A. Game of Life Cellular Automata. Springer London, 2010. 579 p.
4. Ceccherini-Silberstein T., Coornaert M. Cellular Automata and Groups. Springer Berlin Heidelberg, 2010. 440 p.
5. Codd E., Ashenhurst R. Cellular Automata. Academic Press, 1968. 132 p.
6. Gutowitz H. Cellular Automata: Theory and Experiment. MIT Press, 1991. 483 p.
7. Ilachinski A. Cellular Automata: A Discrete Universe. World Scientific, 2001. 808 p.
8. Margenstern M. Small Universal Cellular Automata in Hyperbolic Spaces: A Collection of Jewels. Springer Berlin Heidelberg, 2013. 320 p.
9. McIntosh H. One Dimensional Cellular Automata. Luniver Press, 2009. 280 p.
10. Rosin P., Adamatzky A., Sun X. Cellular Automata in Image Processing and Geometry. Springer International Publishing, 2014. 304 p.
11. Wolfram S. A New Kind of Science. Wolfram Media, 2002. 1192 p.
12. Wolfram S. Cellular automata // Los Alamos Science. 1983. Vol. 9. P. 2–21.
13. Packard N., Wolfram S. Two-dimensional cellular automata // Journal of Statistical Physics. 1985. Vol. 38. P. 901–946.
14. Wolfram S. Cryptography with cellular automata // Lecture Notes in Computer Science. 1986. Vol. 218. P. 429–432.
15. Wolfram S. Cellular automation supercomputing // High-speed computing: scientific applications and algorithm design / Ed. by Robert B. Wilhelmson. University of Illinois Press, 1988. P. 40–48.
16. Wolfram S. Random sequence generation by cellular automata // Advances in Applied Mathematics. 1986. Vol. 7. P. 123–169.
17. Wolfram S. Cellular automata and complexity: collected papers. Addison-Wesley Reading, MA, 1994. Vol. 1. 608 p.
18. Sarkar P. A brief history of cellular automata // Acm computing surveys (csur). 2000. Vol. 32, no. 1. P. 80–107.
19. Schiff J. L. Cellular automata: a discrete view of the world. John Wiley & Sons, 2011. Vol. 45. 272 p.
20. Жуков А. Е. Клеточные автоматы в криптографии. Часть 1 // Вопросы кибербезопасности. 2017. № 3(21). С. 70–76.
21. Кудрявцев В. Б., Подколзин А. С. Об основных направлениях в теории однородных структур // Дискретная математика. 1989. Т. 1, № 3. С. 229–250.
22. Кудрявцев В. Б., Подколзин А. С. Клеточные автоматы. // Интеллектуальные системы. 2006. Т. 10, № 1-4. С. 657–692.
23. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. М.: Наука, 1992. 298 с.
24. Wolfram S. Cellular Automata And Complexity: Collected Papers. CRC Press, 2018. 608 p.
25. Термодинамика необратимых процессов и нелинейная динамика / Е.М. Кольцова, Л.С. Гордеев, Третьяков Ю.Д., Вертегел А.А. М.: Юрлайт, 2019. 430 p.
26. Deutsch A., Dormann S. et al. Cellular automaton modeling of biological pattern formation. Springer, 2005. 464 p.
27. White S. H., Del Rey A. M., Sanchez G. R. Modeling epidemics using cellular automata // Applied mathematics and computation. 2007. Vol. 186, no. 1. P. 193–202.
28. Menshutina N. V., Kolnoochenko A. V., Lebedev E. A. Cellular automata in chemistry and chemical engineering // Annual Review of Chemical and Biomolecular Engineering. 2020. Vol. 11. P. 87–108.
29. Kier L., Seybold P., Cheng C. Modeling Chemical Systems Using Cellular Automata. Springer, 2005. ISBN: 9781402036576.

30. Андреева О. В. Модель и алгоритмы для оценки поврежденности микроструктуры поверхности металлов и сплавов по изображениям: Дис... канд. техн. наук: 05.13.01 / Ольга Вячеславовна Андреева; Нижегор. гос. техн. ун-т им Р.Е. Алексеева. Нижний Новгород, 2017. 162 с.
31. Wagner D. F. Cellular automata and geographic information systems // Environment and planning B: Planning and design. 1997. Vol. 24, no. 2. P. 219–234.
32. Batty M., Xie Y., Sun Z. Modeling urban dynamics through gis-based cellular automata // Computers, environment and urban systems. 1999. Vol. 23, no. 3. P. 205–233.
33. Torrens P. M., O'Sullivan D. Cellular automata and urban simulation: where do we go from here? 2001.
34. Hoekstra A. G., Kroc J., Sloot P. M. Simulating complex systems by cellular automata. Springer, 2010. 384 p.
35. Zuse K. Calculating Space. MIT technical translation. — Massachusetts Institute of Technology, Project MAC, 1970. 188 p.
36. Wolfram S. A Project to Find the Fundamental Theory of Physics. Wolfram Media, Incorporated, 2020. 770 p. ISBN: 9781579550356.
37. Матюшкин И. В., Заплетина М. А. Обзор по тематике клеточных автоматов на базе современных отечественных публикаций // Компьютерные исследования и моделирование. 2019. № 1. С. 9–57.
38. Gardner M. The fantastic combinations of John Conway's new solitaire game ħLifeΛ // Scientific American. 1970. Vol. 223. P. 120–123.
39. Meier W., Staffelbach O. Analysis of pseudo random sequences generated by cellular automata // Workshop on the Theory and Application of of Cryptographic Techniques / Springer. 1991. P. 186–199.
40. Sarkar P. Hiji-bij-bij: A new stream cipher with a self-synchronizing mode of operation // International Conference on Cryptology in India / Springer. 2003. P. 36–51.
41. Joux A., Muller F. Two attacks against the hbb stream cipher // International Workshop on Fast Software Encryption / Springer. 2005. P. 330–341.
42. Karmakar S., Mukhopadhyay D., Chowdhury D. R. Cavium-strengthening trivium stream cipher using cellular automata. // J. Cell. Autom. 2012. Vol. 7, no. 2. P. 179–197.
43. De Canniere C. Trivium: A stream cipher construction inspired by block cipher design principles // Information Security. Springer, 2006. P. 171–186.
44. Das S., Chowdhury D. R. Castream: A new stream cipher suitable for both hardware and software // International Conference on Cellular Automata / Springer. 2012. P. 601–610.
45. Bardell P. H. Analysis of cellular automata used as pseudorandom pattern generators // Proceedings. International Test Conference 1990 / IEEE. 1990. P. 762–768.
46. Fuster-Sabater A., Caballero-Gil P. On the use of cellular automata in symmetric cryptography // Acta Applicandae Mathematica. 2006. Vol. 93, no. 1. P. 215–236.
47. Bouvry P., Seredynski F., Zomaya A. Y. Application of cellular automata for cryptography // International conference on parallel processing and applied mathematics / Springer. 2003. P. 447–454.
48. Tomassini M., Perrenoud M. Cryptography with cellular automata // Applied Soft Computing. 2001. Vol. 1, no. 2. P. 151–160.
49. Henricksen M. A critique of some chaotic-map and cellular automata-based stream ciphers // Annual Asian Computing Science Conference / Springer. 2009. P. 69–78.
50. Bao F. Cryptanalysis of a partially known cellular automata cryptosystem // IEEE Transactions on Computers. 2004. Vol. 53, no. 11. P. 1493–1497.
51. Random number generation — Wolfram Mathematica 7 documentation. Access mode: http://reference.wolfram.com/mathematica/tutorial/RandomNumberGeneration.html.
52. Mukhopadhyay D., RoyChowdhury D. Cellular automata: an ideal candidate for a block cipher // International Conference on Distributed Computing and Internet Technology / Springer. 2004. P. 452–457.
53. Achkoun K., Hanin C., Omary F. SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes // Journal of Discrete Mathematical Sciences and Cryptography. 2020. Vol. 23, No. 8. P. 1529–1544.
54. Seredynski M., Bouvry P. Block encryption using reversible cellular automata // International Conference on Cellular Automata / Springer. 2004. P. 785–792.
55. Seredynski M., Bouvry P. Block cipher based on reversible cellular automata // New Generation Computing. 2005. Vol. 23, No. 3. P. 245–258.
56. Cellular automata based cryptosystem (CAC) / Subhayan Sen, Chandrama Shaw, Dipanwita Roy Chowdhuri et al. // International Conference on Information and Communications Security / Springer. 2002. P. 303–314.
57. Bao F. Cryptanalysis of a new cellular automata cryptosystem // Australasian Conference on Information Security and Privacy / Springer. 2003. P. 416–427.
58. DamgAard I. B. A design principle for hash functions // Conference on the Theory and Application of Cryptology / Springer. 1989. P. 416–427.
59. Daemen J., Govaerts R., Vandewalle J. A framework for the design of one-way hash functions including cryptanalysis of damgAard's one-way function based on a cellular automaton // International Conference on the Theory and Application of Cryptology / Springer. 1991. P. 82–96.
60. HCAHF: A New Family of CA-based Hash Functions / Anas Sadak, Fatima Ezzahra Ziani, Bouchra Echandouri et al. // International Journal of Advanced Computer Science and Applications. 2019. Vol. 10. P. 12.

61. ElRakaiby M. M. Cryptographic hash function using cellular automata // International Journal of Computer Applications Technology and Research. 2016. Vol. 5, No. 5. P. 238–240.
62. Jeon J.-C. Cellular automata based cryptographic hash function // Proceedings of the International Conference on Scientific Computing (CSC) / The Steering Committee of The World Congress in Computer Science, Computer .... 2011. P. 1.
63. Jeon J.-C. One-way hash function based on cellular automata // IT Convergence and Security 2012. Springer, 2013. P. 21–28.
64. 64. Cash: cellular automata based parameterized hash / Sukhendu Kuila, Dhiman Saha, Madhumangal Pal, Dipanwita Roy Chowdhury // International Conference on Security, Privacy, and Applied Cryptography Engineering / Springer. 2014. P. 59–75.
65. Rajeshwaran K., Kumar K. A. Cellular automata based hashing algorithm (cabha) for strong cryptographic hash function // 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) / IEEE. 2019. P. 1–6.
66. A lightweight hash function based on cellular automata for mobile network / Xing Zhang, Qinbao Xu, Xiaowei Li, Changda Wang // 2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN) / IEEE. 2019. P. 247–252.
67. Tanasyuk Y., Perepelitsyn A., Ostapov S. Parameterized fpga-based implementation of cryptographic hash functions using cellular automata // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) / IEEE. 2018. P. 225–228.
68. Sponge functions / Guido Bertoni, Joan Daemen, MichaJel Peeters, Gilles Van Assche // ECRYPT hash workshop / Citeseer. Vol. 2007. 2007.
69. Сухинин Б. М. Применение классических и неоднородных клеточных автоматов при построении высокоскоростных генераторов псевдослучайных последовательностей // Проектирование и технология электронных средств. 2009. № 3. С. 47–51.
70. Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. № 2. С. 34–41.
71. Сухинин Б. М. О влиянии параметров локальной функции связи на распределение значений ячеек двоичных клеточных автоматов // Объединенный научный журнал. 2010. № 8. С. 39–41.
72. Сухинин Б. М. О лавинном эффекте в клеточных автоматах // Объединенный научный журнал. 2010. № 8. С. 41–46.
73. Сухинин Б. М. О новом классе генераторов псевдослучайных последовательностей на основе клеточных автоматов // Объединенный научный журнал. 2010. № 8. С. 46–49.
74. Сухинин Б. М. Практические аспекты оценки качества генераторов случайных последовательностей с равномерным распределением // Объединенный научный журнал. 2010. № 8. С. 49–55.
75. 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. № 8.
76. Сухинин Б. М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2010. № 9.
77. Сухинин Б. М. О некоторых свойствах клеточных автоматов и их применении в структуре генераторов псевдослучайных последовательностей // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2011. № 2. С. 68–76.
78. Сухинин Б. М. Однородные двумерные булевы клеточные автоматы и их свойства применительно к генерации псевдослучайных последовательностей // Системы высокой доступности. 2011. Т. 7, № 2. С. 39–41.
79. Сухинин Б. М. Разработка и исследование высокоскоростных генераторов псевдослучайных равномерно распределенных двоичных последовательностей на основе клеточных автоматов : Дис... канд. техн. наук: 05.13.17 / Борис Михайлович Сухинин: МГТУ им. Н.Э. Баумана. М., 2011. 224 с.
80. Haldar T., Chowdhury D. R. Design of hash function using two dimensional cellular automata // Proceedings of the Fifth International Conference on Mathematics and Computing / Springer. 2021. P. 33–45.
81. Tanasyuk Y., Ostapov S. Development and research of cryptographic hash functions based on two-dimensional cellular automata // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska. 2018. Vol. 8.

CELLULAR AUTOMATA AND THEIR GENERALIZATIONS IN CRYPTOGRAPHY. PART 1

Klyucharev P.G.[3]

The purpose of the article *is an analytical review of the application of cellular automata and their generalizations in cryptography.*

Research method: *an analysis of scientific publications on the topic of the article.*

Results: *The review article analyzes the literature devoted to the use of classical cellular automata and their generalizations for the construction of cryptographic algorithms. The article consists of two parts. The first part is devoted to classical cellular automata and symmetric cryptographic algorithms based on them. It briefly discusses the*

[3] Petr G. Klyucharev, Ph.D., Associate Professor of Information Security department, Bauman Moscow State Technical University, Moscow, Russia. E-mail: pk.iu8@yandex.ru

history of the theory of cellular automata and its applications in various scientific disciplines. The review of the works of a number of authors who proposed symmetric cryptographic algorithms and pseudorandom sequence generators based on one-dimensional cellular automata is presented. The security of such cryptographic algorithms turned out to be insufficient. The following is a review of articles devoted to the use of two-dimensional cellular automata for constructing ciphers (this approach gave the best results). Multidimensional cellular automata are also mentioned. The second part of the article will be devoted to a review of works devoted to the use of generalized cellular automata in cryptography – on the basis of such automata, it is possible to create symmetric encryption algorithms and cryptographic hash functions that provide a high level of security and high performance in hardware implementation (for example, on FPGA), as well as having fairly low requirements for hardware resources. In addition, an attention will be paid to interesting connections of generalized cellular automata, in the context of their use in cryptography, with the theory of expander graphs. Attention will also be paid to the security of cryptographic algorithms based on generalized cellular automata. The works devoted to the implementation of various cryptographic algorithms based on generalized cellular automata on FPGA and GPU will be mentioned. In addition, an overview of asymmetric cryptographic algorithms based on cellular automata will be given. The questions about the belonging of some problems on cellular automata and their generalizations to the class of NP-complete problems, as well as to some other complexity classes, will also be considered.

Keywords: *cellular automation, stream cipher, block cipher, hash function.*

Acknowledgments: The reported study was funded by RFBR, project number 20-17-50258.

References

1. Von Neumann J. The general and logical theory of automata // Proc. Hixon Symposium on Cerebral Mechanisms in Behavior / Ed. by L. A. Jeffress. — New York, 1951. — P. 1–31.
2. Toffoli T., Margolus N. Mashiny kletochnykh avtomatov. — M. : Mir, 1991. — 280 p.
3. Adamatzky A. Game of Life Cellular Automata. — Springer London, 2010. — 579 p.
4. Ceccherini-Silberstein T., Coornaert M. Cellular Automata and Groups. — Springer Berlin Heidelberg, 2010. — 440 p.
5. Codd E., Ashenhurst R. Cellular Automata. — Academic Press, 1968. — 132 p.
6. Gutowitz H. Cellular Automata: Theory and Experiment. — MIT Press, 1991. — 483 p.
7. Ilachinski A. Cellular Automata: A Discrete Universe. — World Scientific, 2001. — 808 p.
8. Margenstern M. Small Universal Cellular Automata in Hyperbolic Spaces: A Collection of Jewels. — Springer Berlin Heidelberg, 2013. — 320 p.
9. McIntosh H. One Dimensional Cellular Automata. — Luniver Press, 2009. — 280 p.
10. Rosin P., Adamatzky A., Sun X. Cellular Automata in Image Processing and Geometry. — Springer International Publishing, 2014. — 304 p.
11. Wolfram S. A New Kind of Science. — Wolfram Media, 2002. — 1192 p.
12. Wolfram S. Cellular automata // Los Alamos Science. — 1983. — Vol. 9. — P. 2–21.
13. Packard N., Wolfram S. Two-dimensional cellular automata // Journal of Statistical Physics. — 1985. — Vol. 38. — P. 901–946.
14. Wolfram S. Cryptography with cellular automata // Lecture Notes in Computer Science. — 1986. — Vol. 218. — P. 429–432.
15. Wolfram S. Cellular automation supercomputing // High-speed computing: scientific applications and algorithm design / Ed. by Robert B. Wilhelmson. — University of Illinois Press, 1988. — P. 40–48.
16. Wolfram S. Random sequence generation by cellular automata // Advances in Applied Mathematics. — 1986. — Vol. 7. — P. 123–169.
17. Wolfram S. Cellular automata and complexity: collected papers. — Addison-Wesley Reading, MA, 1994. — Vol. 1. — 608 p.
18. Sarkar P. A brief history of cellular automata // Acm computing surveys (csur). — 2000. — Vol. 32, no. 1. — P. 80–107.
19. Schiff J. L. Cellular automata: a discrete view of the world. — John Wiley & Sons, 2011. — Vol. 45. — 272 p.
20. Zhukov A. E. Kletochnye avtomaty v kriptografii. Chast' 1 // Voprosy kiberbezopasnosti. — 2017. — № 3(21). — P. 70–76.
21. Kudryavtsev V. B., Podkolzin A. S. Ob osnovnykh napravleniyakh v teorii odnorodnykh struktur // Diskretnaya matematika. — 1989. — T. 1, № 3. — P. 229–250.
22. Kudryavtsev V. B., Podkolzin A. S. Kletochnye avtomaty. // Intellektual'nye sistemy. — 2006. — T. 10, № 1-4. — P. 657–692.
23. Kudryavtsev V. B., Podkolzin A. S., Bolotov A. A. Osnovy teorii odnorodnykh struktur. — M.: Nauka, 1992. — 298 p.
24. Wolfram S. Cellular Automata And Complexity: Collected Papers. — CRC Press, 2018. — 608 p.
25. Termodinamika neobratimykh protsessov i nelineinaya dinamika / E.M. Kol'tsova, L.S. Gordeev, Tret'yakov Yu.D., Vertegel A.A. — M.: Yurlait, 2019. — 430 p.
26. Deutsch A., Dormann S. et al. Cellular automaton modeling of biological pattern formation. — Springer, 2005. — 464 p.
27. White S. H., Del Rey A. M., Sanchez G. R. Modeling epidemics using cellular automata // Applied mathematics and computation. — 2007. — Vol. 186, no. 1. — P. 193–202.
28. Menshutina N. V., Kolnoochenko A. V., Lebedev E. A. Cellular automata in chemistry and chemical engineering // Annual Review of Chemical and Biomolecular Engineering. — 2020. — Vol. 11. — P. 87–108.
29. Kier L., Seybold P., Cheng C. Modeling Chemical Systems Using Cellular Automata. — Springer, 2005. — ISBN: 9781402036576.

30. Andreeva O. V. Model' i algoritmy dlya otsenki povrezhdennosti mikrostruktury poverkhnosti metallov i splavov po izobrazheniyam : Dis... kand. tekhn. nauk: 05.13.01 / Ol'ga Vyacheslavovna Andreeva ; Nizhegor. gos. tekhn. un-t im R.E. Alekseeva. — Nizhnii Novgorod, 2017. — 162 p.
31. Wagner D. F. Cellular automata and geographic information systems // Environment and planning B: Planning and design. — 1997. — Vol. 24, no. 2. — P. 219–234.
32. Batty M., Xie Y., Sun Z. Modeling urban dynamics through gis-based cellular automata // Computers, environment and urban systems. — 1999. — Vol. 23, no. 3. — P. 205–233.
33. Torrens P. M., O'Sullivan D. Cellular automata and urban simulation: where do we go from here? — 2001.
34. Hoekstra A. G., Kroc J., Sloot P. M. Simulating complex systems by cellular automata. — Springer, 2010. — 384 p.
35. Zuse K. Calculating Space. MIT technical translation. — Massachusetts Institute of Technology, Project MAC, 1970. — 188 p.
36. Wolfram S. A Project to Find the Fundamental Theory of Physics. — Wolfram Media, Incorporated, 2020. — 770 p. — ISBN: 9781579550356.
37. Matyushkin I. V., Zapletina M. A. Obzor po tematike kletochnykh avtomatov na baze sovremennykh otechestvennykh publikatsii // Komp'yuternye issledovaniya i modelirovanie. — 2019. — № 1. — P. 9–57.
38. Gardner M. The fantastic combinations of John Conway's new solitaire game ħLifeL // Scientific American. — 1970. — Vol. 223. — P. 120–123.
39. Meier W., Staffelbach O. Analysis of pseudo random sequences generated by cellular automata // Workshop on the Theory and Application of of Cryptographic Techniques / Springer. — 1991. — P. 186–199.
40. Sarkar P. Hiji-bij-bij: A new stream cipher with a self-synchronizing mode of operation // International Conference on Cryptology in India / Springer. — 2003. — P. 36–51.
41. Joux A., Muller F. Two attacks against the hbb stream cipher // International Workshop on Fast Software Encryption / Springer. — 2005. — P. 330–341.
42. Karmakar S., Mukhopadhyay D., Chowdhury D. R. Cavium-strengthening trivium stream cipher using cellular automata. // J. Cell. Autom. — 2012. — Vol. 7, no. 2. — P. 179–197.
43. De Canniere C. Trivium: A stream cipher construction inspired by block cipher design principles // Information Security. — Springer, 2006. — P. 171–186.
44. Das S., Chowdhury D. R. Castream: A new stream cipher suitable for both hardware and software // International Conference on Cellular Automata / Springer. — 2012. — P. 601–610.
45. Bardell P. H. Analysis of cellular automata used as pseudorandom pattern generators // Proceedings. International Test Conference 1990 / IEEE. — 1990. — P. 762–768.
46. Fuster-Sabater A., Caballero-Gil P. On the use of cellular automata in symmetric cryptography // Acta Applicandae Mathematica. — 2006. — Vol. 93, no. 1. — P. 215–236.
47. Bouvry P., Seredynski F., Zomaya A. Y. Application of cellular automata for cryptography // International conference on parallel processing and applied mathematics / Springer. — 2003. — P. 447–454.
48. Tomassini M., Perrenoud M. Cryptography with cellular automata // Applied Soft Computing. — 2001. — Vol. 1, no. 2. — P. 151–160.
49. Henricksen M. A critique of some chaotic-map and cellular automata-based stream ciphers // Annual Asian Computing Science Conference / Springer. — 2009. — P. 69–78.
50. Bao F. Cryptanalysis of a partially known cellular automata cryptosystem // IEEE Transactions on Computers. — 2004. — Vol. 53, no. 11. — P. 1493–1497.
51. Random number generation — Wolfram Mathematica 7 documentation. — Access mode: http://reference.wolfram.com/mathematica/tutorial/RandomNumberGeneration.html.
52. Mukhopadhyay D., RoyChowdhury D. Cellular automata: an ideal candidate for a block cipher // International Conference on Distributed Computing and Internet Technology / Springer. — 2004. — P. 452–457.
53. Achkoun K., Hanin C., Omary F. SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes // Journal of Discrete Mathematical Sciences and Cryptography. — 2020. — Vol. 23, no. 8. — P. 1529–1544.
54. Seredynski M., Bouvry P. Block encryption using reversible cellular automata // International Conference on Cellular Automata / Springer. — 2004. — P. 785–792.
55. Seredynski M., Bouvry P. Block cipher based on reversible cellular automata // New Generation Computing. — 2005. — Vol. 23, no. 3. — P. 245–258.
56. Cellular automata based cryptosystem (CAC) / Subhayan Sen, Chandrama Shaw, Dipanwita Roy Chowdhuri et al. // International Conference on Information and Communications Security / Springer. — 2002. — P. 303–314.
57. Bao F. Cryptanalysis of a new cellular automata cryptosystem // Australasian Conference on Information Security and Privacy / Springer. — 2003. — P. 416–427.
58. DamgAard I. B. A design principle for hash functions // Conference on the Theory and Application of Cryptology / Springer. — 1989. — P. 416–427.
59. Daemen J., Govaerts R., Vandewalle J. A framework for the design of one-way hash functions including cryptanalysis of damgAard's one-way function based on a cellular automaton // International Conference on the Theory and Application of Cryptology / Springer. — 1991. — P. 82–96.

60. HCAHF: A New Family of CA-based Hash Functions / Anas Sadak, Fatima Ezzahra Ziani, Bouchra Echandouri et al. // International Journal of Advanced Computer Science and Applications. — 2019. — Vol. 10. — P. 12.
61. ElRakaiby M. M. Cryptographic hash function using cellular automata // International Journal of Computer Applications Technology and Research. — 2016. — Vol. 5, no. 5. — P. 238–240.
62. Jeon J.-C. Cellular automata based cryptographic hash function // Proceedings of the International Conference on Scientific Computing (CSC) / The Steering Committee of The World Congress in Computer Science, Computer .... — 2011. — P. 1.
63. Jeon J.-C. One-way hash function based on cellular automata // IT Convergence and Security 2012. — Springer, 2013. — P. 21–28.
64. Cash: cellular automata based parameterized hash / Sukhendu Kuila, Dhiman Saha, Madhumangal Pal, Dipanwita Roy Chowdhury // International Conference on Security, Privacy, and Applied Cryptography Engineering / Springer. — 2014. — P. 59–75.
65. Rajeshwaran K., Kumar K. A. Cellular automata based hashing algorithm (cabha) for strong cryptographic hash function // 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) / IEEE. — 2019. — P. 1–6.
66. A lightweight hash function based on cellular automata for mobile network / Xing Zhang, Qinbao Xu, Xiaowei Li, Changda Wang // 2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN) / IEEE. — 2019. — P. 247–252.
67. Tanasyuk Y., Perepelitsyn A., Ostapov S. Parameterized fpga-based implementation of cryptographic hash functions using cellular automata // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) / IEEE. — 2018. — P. 225–228.
68. Sponge functions / Guido Bertoni, Joan Daemen, MichaJel Peeters, Gilles Van Assche // ECRYPT hash workshop / Citeseer. — Vol. 2007. — 2007.
69. Sukhinin B. M. Primenenie klassicheskikh i neodnorodnykh kletochnykh avtomatov pri postroenii vysokoskorostnykh generatorov psevdosluchainykh posledovatel'nostei // Proektirovanie i tekhnologiya elektronnykh sredstv. — 2009. — № 3. — P. 47–51.
70. Sukhinin B. M. Vysokoskorostnye generatory psevdosluchainykh posledovatel'nostei na osnove kletochnykh avtomatov // Prikladnaya diskretnaya matematika. — 2010. — № 2. — P. 34–41.
71. Sukhinin B. M. O vliyanii parametrov lokal'noi funktsii svyazi na raspredelenie znachenii yacheek dvoichnykh kletochnykh avtomatov // Ob"edinennyi nauchnyi zhurnal. — 2010. — № 8. — P. 39–41.
72. Sukhinin B. M. O lavinnom effekte v kletochnykh avtomatakh // Ob"edinennyi nauchnyi zhurnal. — 2010. — № 8. — P. 41–46.
73. Sukhinin B. M. O novom klasse generatorov psevdosluchainykh posledovatel'nostei na osnove kletochnykh avtomatov // Ob"edinennyi nauchnyi zhurnal. — 2010. — № 8. — P. 46–49.
74. Sukhinin B. M. Prakticheskie aspekty otsenki kachestva generatorov sluchainykh posledovatel'nostei s ravnomernym raspredeleniem // Ob"edinennyi nauchnyi zhurnal. — 2010. — № 8. — P. 49–55.
75. Sukhinin B. M. Issledovanie kharakteristik lavinnogo effekta v dvoichnykh kletochnykh avtomatakh s ravnovesnymi funktsiyami perekhodov // Nauka i obrazovanie. MGTU im. N.E. Baumana. Elektron. zhurn. — 2010. — № 8.
76. Sukhinin B. M. Razrabotka generatorov psevdosluchainykh dvoichnykh posledovatel'nostei na osnove kletochnykh avtomatov // Nauka i obrazovanie. MGTU im. N.E. Baumana. Elektron. zhurn. — 2010. — № 9.
77. Sukhinin B. M. O nekotorykh svoistvakh kletochnykh avtomatov i ikh primenenii v strukture generatorov psevdosluchainykh posledovatel'nostei // Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya: Priborostroenie. — 2011. — № 2. — P. 68–76.
78. Sukhinin B. M. Odnorodnye dvumernye bulevy kletochnye avtomaty i ikh svoistva primenitel'no k generatsii psevdosluchainykh posledovatel'nostei // Sistemy vysokoi dostupnosti. — 2011. — T. 7, № 2. — P. 39–41.
79. Sukhinin B. M. Razrabotka i issledovanie vysokoskorostnykh generatorov psevdosluchainykh ravnomerno raspredelennykh dvoichnykh posledovatel'nostei na osnove kletochnykh avtomatov : Dis... kand. tekhn. nauk: 05.13.17 / Boris Mikhailovich Sukhinin ; MGTU im. N.E. Baumana. — M., 2011. — 224 p.
80. Haldar T., Chowdhury D. R. Design of hash function using two dimensional cellular automata // Proceedings of the Fifth International Conference on Mathematics and Computing / Springer. — 2021. — P. 33–45.
81. Tanasyuk Y., Ostapov S. Development and research of cryptographic hash functions based on two-dimensional cellular automata // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska. — 2018. — Vol. 8.