ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.55 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait.2021.2/3506
Поступила в редакцию 12.03.2021
Подписана в печать 19.07.2021

МЕТОДЫ ПРИМЕНЕНИЯ КЛЕТОЧНЫХ АВТОМАТОВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

© 2021 Е. А. Кулешова✉

Юго-Западный государственный университет
ул. Челюскинцев, 19, корпус Б, 305004 Курск, Российская Федерация

Аннотация. В данной статье проведен обзор автоматных шифраторов, основанных на клеточных автоматах, областью применения которых являются системы защиты информации. Рассмотрены исследования, посвященные вариантам применения клеточных автоматов в системах симметричного шифрования и их практической реализации, а также вариантам построения криптосистем с открытым ключом на основе клеточных автоматов, использованию клеточных автоматов для генерации псевдослучайных чисел, а также исследования, в которых представлены методы построения криптографических хэш-функций с использованием клеточных автоматов. Представлено обобщенное понятие абстрактного автомата и более усовершенствованных моделей клеточных автоматов, проведен сравнительный обзор моделей клеточных автоматов с целевой функцией и клеточных автоматов с плавающим окном, включающий описание алгоритмов их работы и некоторую оценку стойкости. Рассмотрены методы применения клеточных автоматов при многопоточной обработке данных с возможностью применении паттернов, определяющих индивидуальную окрестность элементов при клеточном шифровании, и возможностью использования справочника, содержащего набор правил обхода матрицы шифрования, а также метод одноключевого преобразования двоичных потоков данных с открытым параметром на базе клеточного автомата с плавающим окном и динамической матрицей, разделяющейся на элементарные сегменты. Рассмотрена возможность применения клеточных автоматов при многопоточной обработке данных в режиме реального времени. В заключении приведены рекомендации по повышению стойкости методов защиты информации, основанных на клеточных автоматах, одним из которых является метод использования расширенного ключа, определяющего псевдослучайную окрестность, с учетом положения обрабатываемого бита в матрице исходных данных.
Ключевые слова: клеточный автомат, последовательный автоматный шифратор, клеточный автомат с целевой функцией, клеточный автомат с плавающим окном, клеточный автомат на разбиении, защита конфиденциальной информации, информационная безопасность, преобразование данных.

ВВЕДЕНИЕ

Идея клеточных автоматов была независимо сформулирована Дж. фон Нейманом и К. Цуссе. Клеточные автоматы (КА) рассматривались в качестве универсальной вычислительной среды, предназначенной для моделирования физических процессов и построения алгоритмов, и являлась эквивалентной по своим вычислительным возможностям машине Тьюринга. На основе этой идеи были проведены многочисленные теоретические и прикладные исследования. Начиная с 70-х

✉ Кулешова Елена Александровна
e-mail: lena.kuleshova.94@mail.ru

годов в Берлине стали регулярно проводиться конференции международного уровня по параллельной обработке информации на КА [1].

Наибольшее распространение КА получили в области симметричного шифрования [2–5], сжатия данных [6, 7], обработке изображений [8, 9], также КА получили широкое распространение в медицине.

В области шифрования данных следует отметить исследования, приведенные в работе [10], в которой было предложено семейство блочных шифров, построенных с использованием обобщенных КА на основе семейства псевдослучайных функций. КА обладают свойством перехода состояний, что является основой для определения фундаментальных преобразований в системе шифрования. На основании этого в работе [11] предложен вариант блочного шифра с симметричным ключом на основе КА, суть которого состоит в использовании различных конфигураций правил КА для формирования гибридных обратимых КА, которые в свою очередь используются при шифровании и дешифровании данных. Механизм использования гибридных КА также рассмотрен в работе [12] на примере динамической системы, использующей данных механизм для достижения обратимости, адаптированной для построения блочного шифра. В работах [13, 14] предложен блочный шифр на основе КА, который объединяет сети замещения-перестановки (SPN) со схемой Фейстеля с использованием S-блоков, зависящих от ключа, интересной особенностью которого является использование набора правил, сочетающего линейные и нелинейные правила КА. Вопросы практической реализации, оценки производительности и области применения блочных шифров, основанных на КА, рассмотрены в работе [15], разработка программного обеспечения блочного шифра на основе обратимых КА и исследование его статистических свойств представлены в работе [16].

Большинство исследований криптосистем на основе КА сосредоточено на традиционных криптосистемах с секретным ключом, однако существуют варианты построения криптосистем с открытым ключом на основе КА. Теоретические аспекты построения систем с открытым ключом на основе обратимых КА изложены в работе [17], однако остается нерешенным вопрос реализации алгоритма генерации ключей. В работе [18] авторы доказывают, что при определенных предположениях маркер КА имеет единственный обратный элемент с заданной окрестностью, и они используют результат для разработки алгоритма генерации рабочего ключа для шифрования с открытым ключом на основе обратимого КА. Алгоритм, позволяющий построить на базе КА систему преобразования данных с открытым ключом, предложен в работе [19], данный алгоритм использует 4 одномерных обратимых КА в качестве секретного ключа для построения двумерного КА окрестности Мура, который принимается в качестве открытого ключа. Данные схемы основаны на функции лазейки, которая обеспечивает только одностороннюю безопасность, и могут не удовлетворять требованиям безопасности при атаках по выбранному открытому тексту.

Основываясь на том, что КА имеет множество характеристик, таких как простые правила составных единиц, локальная связность единиц, высокая степень параллелизма в обработке информации и сложные характеристики глобальных функций в работах [20, 21] представлены варианты построения генераторов псевдослучайных чисел на основе КА. Использование свойств КА для генерации псевдослучайных чисел также нашло отображение в работе [22], предложенный в данной работе метод основан на использовании правил переходов ячеек КА и шаблонов соседства. Подробный обзор применения КА, в том числе неоднородных КА для построения псевдослучайных чисел был проведен в работе [23].

Также довольно широкое распространение получило использование КА при построении хэш-функций, это связано с тем, что криптографические хэш-функции играют важную роль в сфере информационной безопасности, так в работах [24, 25] были предложены методы построения криптографических хэш-функций с использованием

обобщенных КА и описана возможность их использования в качестве функций формирования ключей. В работе [26] был предложен алгоритм хеширования на основе КА, использующий правила КА и настраиваемую функцию преобразования для создания хэша из входного сообщения и ключа. Использование КА подразумевает ограничения по количеству используемых правил и длине отдельных последовательностей состояний, в работе [27] было предложено решение данной проблемы за счет использования неоднородных КА.

В данной статье приведен обзор автоматных шифраторов, получивших применение в области обработки (шифрования) данных, а также моделей шифрования, основанных на КА, применяемых в многопоточных системах обработки данных, работающих в режиме реального времени.

1. МЕТОДЫ И МАТЕРИАЛЫ ИССЛЕДОВАНИЯ

Клеточный автомат состоит из набора ячеек, организованных в виде регулярной сети. Каждая ячейка КА — это конечный автомат, который использует множество конечных состояний X'. КА развиваются в дискретном времени и пространстве. В процессе эволюции клетка КА меняет свое состояние в зависимости от текущих состояний своих соседей. То есть, чтобы обновить свое состояние, ячейка использует функцию следующего состояния, также известную как локальное правило, аргументы которой являются текущими состояниями соседей ячейки. Сбор состояний всех ячеек в данный момент времени называется конфигурацией КА. Следовательно, в процессе эволюции КА перескакивает от одной конфигурации к другой. Обратимость КА программируется с помощью выбора локального правила обновления.

КА — это модель, описываемая кортежем:

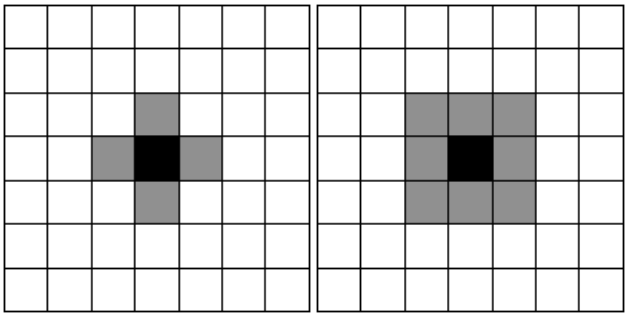
$$A = (Z, X, N, f), \qquad (1)$$

где $Z \subseteq Z^n$ — n-мерное клеточное пространство; X — множество конечных состояний; $N = (\vec{n}_1, \vec{n}_2, ...\vec{n}_N)$ — вектор окрестности различных элементов Z, который связывает одну клетку со своими соседями. Обычно соседи ячейки — это ближайшие ячейки, окружающие ячейку. Однако, когда задан вектор окрестности N, то соседи ячейки в местоположении $\vec{n}_1 \in Z$ находятся в точках $(\vec{n} + \vec{n}_i) \in Z$ для всех $i \in \{1, 2, ..., N\}$. Функция $f : X^N \to X$ называется локальным правилом автомата. Следующее состояние клетки задается функцией $f(a_1, a_2, ..., a_N)$, где $a_1, a_2, ..., a_N$ — это состояние ее N соседей.

Окрестности ячеек КА сильно коррелируют с размером КА. Исходный КА, предложенный фон Нейманом, является двумерным и использует зависимость из 5 соседей (ортогональную и саму). На рис. 1(а) представлена такая зависимость: соседями ячейки является сама центральная ячейка и четыре заштрихованные ячейки. Традиционная данная зависимость называется окрестностью фон Неймана первого порядка.

Естественным расширением этой зависимости ячейки КА от ее соседей является зависимость из 9 соседей, где четыре неортогональные ячейки дополнительно рассматриваются как соседи. На рис. 1(б) показан такой вид зависимости, который был предложен Муром (1962) и традиционно известен как окрестность Мура. Данная структура была использована при разработке знаменитой Игры Жизнь.

В зависимости от выбранной окрестности количество различных вариантов обхода также будет меняться. Так, для окрестности Мура первого порядка существует 8! различных

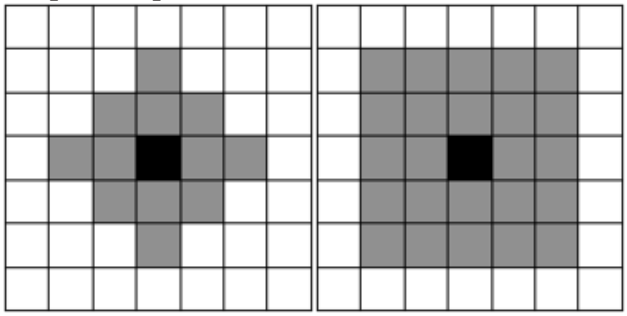


а) *б)*

Рис.1. (а) Окрестность фон Неймана первого порядка; (б) окрестность Мура первого порядка

Fig. 1. (a) First-Order Von Neumann Neighborhood; (b) First-Order Moore Neighborhood

вариантов обхода, для окрестности Фон Неймана первого порядка – 4! различных вариантов обхода (в обеих окрестностях мы не учитываем центральную клетку, т.к. она не влияет на стойкость). На рис. 2(а) и 2(б) представлены окрестности фон Неймана и Мура второго порядка.



а) *б)*

Рис.2. (а) Окрестность фон Неймана второго порядка; (б) окрестность Мура второго порядка
Fig. 2. (a) Second-order Von Neumann Neighborhood; (b) Second-order Moore Neighborhood

КА также идентифицируется по его глобальной функции переходов. Пусть C представляет собой множество всех конфигураций X^Z. Тогда КА — это функция $F : C \to C$, которая называется глобальной функцией переходов. В классическом представлении КА являются синхронными (то есть все ячейки обновляются одновременно) и однородными (то есть все ячейки используют одну функцию следующего состояния). Тем не менее, КА описывается четырьмя параметрами Z, X, N, f. На протяжении многих лет предлагались различные модели КА, варьирующие свойства этих параметров, некоторые из которых будут рассмотрены в данной статье.

2.1. Клеточный автомат с целевой функцией

Одним из наиболее популярных направлений в области преобразования данных с применением КА является шифрование конфиденциальных данных. С точки зрения теории автоматов блочный шифратор с длиной блока k, $(k = 64, 128, 256, \ldots)$ — это конечный автомат с k состояниями. При этом автомат наследует все недостатки первого типа шифрования. Это связано с тем, при блочном преобразовании возникает необходимость разбиения исходной информации на блоки заданного размера, каждый из которых обрабатывается отдельно, что в свою очередь ведет к увеличению времени преобразования конфиденциальной информации. Основной проблемой является отсутствие возможности перехода к следующему блоку информации до окончания обработки текущего блока информации. В работе [28] была рассмотрена возможность решения данной проблемы за счет введения ограничений при переходе от блочного шифрования к поточному и предложено понятие последовательного КА:

Последовательным КА называется кортеж из 5-ти элементов:

$$CA_s = \langle Z, X, N, q_0, \delta \rangle, \qquad (2)$$

где q_0 — начальное состояние; δ — функция переходов.

Следует отметить, что данная модель требует соблюдения ряда критериев для обеспечения обратимости. Более подробно вопрос обратимости КА рассмотрен в работе [17].

Каждая ячейка (клетка) КА содержит несколько битов данных и на каждом шаге связана с соседними клетками посредством обмена информацией. Клетки меняют свое состояние синхронно с дискретными временными шагами. Следующее состояние каждой ячейки зависит от текущего состояния соседних ячеек в соответствии с правилом обновления. Все ячейки КА используют одно и то же правило, и правило применяется ко всем ячейкам одновременно. Однако, соседние ячейки КА могут быть ближайшими ячейками, окружающими ячейку, но можно указать более общие окрестности, задав относительные смещение соседей. На основе этого в работе [29] дается описание КА с целевой функцией. Данная идея получила развитие в работе [30], в которой была представлена усовершенствованная модель КА с целевой функцией. При этом шифрование производится следующим образом: выполняется операция *XOR* (сложение по модулю «два») содержания центральной клетки с содержанием тех клеток соответствующей окрестности, для которых соответствую-

щий элемент ключа ненулевой. Также необходимо отметить, что шифрование производится динамически, т.е. значение клетки, полученное на предыдущем шаге, будет влиять на значения соседних клеток на последующих шагах.

В исходном определении КА на разбиении, данном в работе [29], подразумевается обход блока шифрования, начиная с первого элемента и далее по порядку строк и соответственно столбцов, но для повышения стойкости клеточного шифрования обход можно совершать в любой последовательности. На основании этого в работе [31] был введен новый элемент L — маршрут обхода блока шифрования КА и приведено определение усовершенствованного КА на разбиении.

КА на разбиении называется 7-ка:

$$CA_p = \langle Z^n, (N_1, ..., N_n), A, (m_1, ..., m_n), S, \Psi, L \rangle, \quad (3)$$

где Z^n — размерность КА $n = 1, 2, 3$; $(N_1, ..., N_n)$ — размер таблицы; A — алфавит внутренних состояний; $(m_1, ..., m_n)$ — размер блока преобразования данных; S — порядок разбиения КА на блоки, подлежащие преобразованию; Ψ — перечень значений функций переходов; L — маршрут обхода преобразуемого блока.

При шифровании КА на разбиении исходный текст построчно располагается в таблице исходного текста. Далее таблица исходного текста разбивается на блоки нечетной решетки, после чего блок шифрования раскрывается в строку и ему сопоставляется строка в соответствии с функцией переходов, после чего происходит замена исходного блока на преобразованный. Шифрование проводится по всей таблице, затем матрица шифруемого текста разбивается на блоки четной решеткой и процесс повторяется. При этом первый и последний столбцы таблицы шифрования дополняются до нужного числа столбцов клетки разбиения торообразным замыканием всей таблицы шифрования. При дешифровании применяется тот же алгоритм, но меняется очередность разбиения на блоки нечетной и четной решеткой, а в таблице функций переходов столбцы меняются местами. Количество шагов при дешифровании должно быть таким же, как при шифровании.

С целью повышения стойкости КА в работе [32] была предложена новая модель КА с плавающим окном. Основным отличием КА с плавающим окном от КА на разбиении является то, что отсутствует разделение на блоки шифрования четной и нечетной решетками. Еще одной особенностью является то, что сеанс шифрования предполагает последовательный обход элементов матрицы, являющейся отражением данных в открытом виде и применение к ним правила обхода. При этом смещение происходит на один столбец, за счет чего шифрование происходит в несколько слоев, что обеспечивает потенциальную возможность проведения нескольких раундов обработки элемента матрицы (с целью обеспечения более высокого уровня защищенности данных). Дешифрование включает в себя обратный обход матрицы, что позволяет обеспечить обратимость преобразования.

2.2. Усовершенствованные модели клеточных автоматов

Идея КА с плавающим окном получила развитие в работе [33], в которой была предложена система многопоточной обработки данных на основе КА с плавающим окном.

При клеточном преобразовании данного типа появляется возможность произвольно задать размер блока шифрования $m_1 \times m_2$, в зависимости от которого будет программно определено количество столбцов матрицы. Количество строк матрицы определяется размером исходных данных, а в случае сетевого потока зависит от сеанса взаимодействия пользователей компьютерной сети [34]. Число столбцов N_2 зависит от длины исходной информации и определяется по формуле 4:

$$N_2 = qm_2 + 1, \quad (4)$$

где q — неполное частное в равенстве $T = kq + r, 0 \le r < k, k = m_1 \times m_2$ — размер блока шифрования, T — длина исходного текста, а r — неполное частное.

В работе [35] предлагается новый метод одноключевого преобразования двоичных потоков данных с открытым параметром на базе КА с плавающим окном и динамической

матрицей, разделяющейся на элементарные сегменты. Открытым параметром является число столбцов информационной матрицы — эта информация передается по открытому каналу связи. Закрытый ключ состоит из матрицы шифрования и правила обхода матрицы данных. Также в данной работе предложена математическая модель формирования уникальных характеристик данных, основанная на применении шаблонов (паттернов), определяющих индивидуальную окрестность элементов при клеточном шифровании.

КА с псевдослучайной окрестностью (ПСО) и набором паттернов называется совокупность, представленная ниже:

$$CA_{OP} = \langle Z^n, (N_1, ..., N_n), A, P, (p_1, ..., p_n), X, Slide \rangle, \quad (5)$$

где Z^n — размерность КА $n = 1, 2, 3$; $(N_1, ..., N_n)$ — размер сегмента матрицы данных, при этом N_1 является открытым параметром шифрования; $A = \{0,1\}$ — значение битов данных; $P(p_1, ..., p_n)$ — шифр-матрица (паттерн); X — размерность матрицы шифрования; $Slide$ — правило обхода элементов информационной матрицы при обработке.

Процесс шифрования при этом состоит в следующем. В соответствии с правилом обхода матрицы $Slide$ берется текущий бит обрабатываемого сегмента матрицы данных. Определяется координата центра ПСО, по единичным значениям бит которого определяются задействованные в преобразовании текущего бита данных соседи. Обработка текущего элемента заключается в применении логической операции «исключающее или» к множеству ячеек, принадлежащих активной окрестности обрабатываемого элемента матрицы в соответствии с паттерном $p \in P$.

На рис. 3 показан вариант шаблона (патерна), включающий центральный (обрабатываемый) и 4 элемента из окружения. Для удобства ввода ключей и взаимодействия пользователей системы ключ задается последовательностью идентификаторов, определяющих расположение элемента в окрестности P. Формальная запись указанного на рисунке паттерна может быть упрощенно представлена последовательностью EGJL или математически формулой 6:

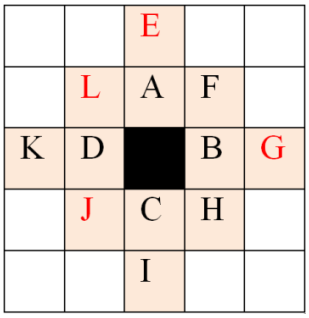


Рис. 3. Пример шаблона для окрестности фон Неймана 2-го порядка
Fig. 3. An example of a template for a second-order von Neumann neighborhood

$$P = p_{x,y} \oplus p_{x,y+2} \oplus p_{x+2,y} \oplus p_{x-1,y-1} \oplus p_{x-1,y+1}. \quad (6)$$

Таким образом, при движении по сегменту происходит движение по матрице-шифру. В связи с тем, что расширение матрицы по периметру не требуется — выполняется логическая операция XOR текущего бита матрицы и единичных бит из существующих (с учетом границ обрабатываемого сегмента) и отмеченных правилом ПСО. В случае если результат, полученный на предыдущем действии, отличается от значения текущего бита – производится его инверсия. Если не весь сегмент обработан, то выполняется переход к следующему биту в соответствии с правилом обхода. Обработанная цепочка бит в виде матрицы-результата выгружается в выходной буфер, на этом обработка завершена. Признак обработки всего потока данных устанавливается в истину, когда все сегменты, созданные на уровне планировщика задачи, обработаны.

Отдельно стоит отметить возможность использования справочника, содержащего набор правил обхода матрицы. На рис. 4 представлен вариант наполнения справочника Slide. В данный справочник также можно включить обход матрицы по правилу Варнсдорфа, поскольку обход по данному правилу положительно сказывается на времени обработки каждого блока, однако, данное правило применимо лишь в частных случаях из-за необходимости разбиения матрицы на строго квадратные блоки.

Использование данного справочника можно позволяет ввести несколько уровней защиты, например, базовый уровень защиты

A			B			C			D			E			F		
1	2	3	3	2	1	1	4	7	7	4	1	1	2	3	3	2	1
4	5	6	6	5	4	2	5	8	8	5	2	8	9	4	4	9	8
7	8	9	9	8	7	3	6	9	9	6	3	7	6	5	5	6	7

• • •

U			V			W			X			Y			Z		
1	2	6	6	2	1	9	8	4	6	7	9	1	6	2	5	9	4
3	5	7	7	5	3	7	5	3	2	5	8	7	3	8	8	3	7
4	8	9	9	8	4	6	2	1	1	3	4	4	9	5	2	6	1

Рис. 4. Вариант наполнения справочника Slide
Fig. 4. Option to Fill the Slide Directory

будет предполагать однократный обход элементов матрицы по выбранному маршруту, а продвинутый уровень защиты — два варианта обхода, что позволит добиться большего уровня защищенности конфиденциальных данных при их преобразовании.

Преимущество метода состоит в гибкости и высокой скорости обработки данных при сохранении достаточной стойкости.

В ходе исследований сопоставлены метод преобразования конфиденциальных данных на основе КА с плавающим окном (оригинальный) и метод на основе КА с использованием паттернов (модифицированный). На рис. 5 представлены графики сравнения скорости обработки данных одним потоком. Для объективности результатов с учетом длины потока данных — группа экспериментов разделена на два этапа: обработка последовательностей менее 10 Мб (графика, документы, аудиофайлы), и превышающих это значение (видео-контент, архивы и т. д.). Все эксперименты проводились на одном и том же оборудовании.

Из рис. 5 видно, что быстродействие модифицированного метода остается на уровне оригинального, а при обработке больших потоков данных имеет меньшие отклонения от средней величины. Это позволяет прогнозировать время обработки и учитывать при подборе аппаратной части.

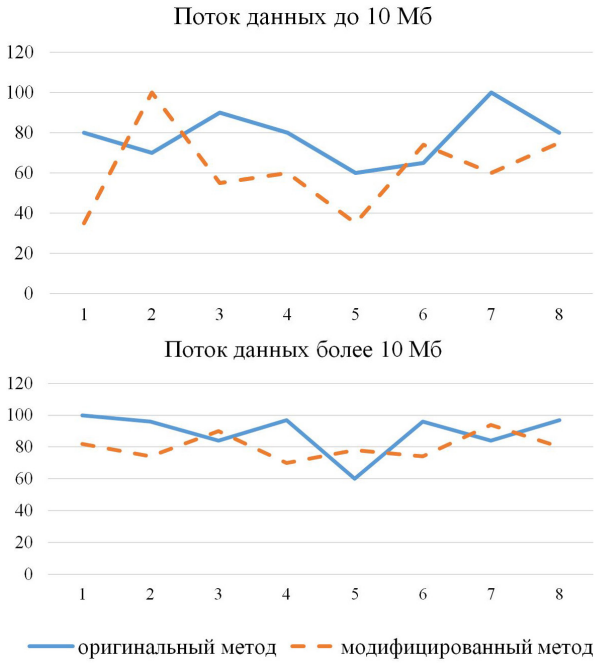


Рис. 5. Относительные задержки с привязкой к методу преобразования
Fig. 5. Relative Delays with Reference to the Conversion Method

3. РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Важной особенностью усовершенствованных моделей КА является введение правил, позволяющих обход блока шифрования в любой последовательности. В то время как в классическом КА на разбиении обход блока шифрования начинается по умолчанию с первого элемента и далее по порядку строк и соответственно столбцов.

Введение подобного правила положительно сказывается на стойкости шифрования. Допустим размер блока шифрования $M * N$, тогда количество вариантов обхода данного блока будет $(M * N)!$. Таким образом, вероятность угадывания «маршрута» обхода блока шифрования равна $1/(M * N)!$

Также стоит отметить, что в усовершенствованных методах появилось возможность выбора размера блока шифрования, от которого зависит таблица функций переходов. Так при увеличении размера блока шифрования в геометрической прогрессии растет количество вариантов заполнения правой части таблицы (функций переходов), следовательно, усложняется задача вскрытия шифра. Но необходимо учитывать, что увеличение блока шифрования возможно только при шифровании больших сообщений.

При многопоточной обработке данных на основе КА (в целях повышения уровня защищенности конфиденциальных данных при их преобразовании) целесообразно использование расширенного ключа, определяющего псевдослучайную окрестность, с учетом положения обрабатываемого бита в матрице исходных данных. При этом на обрабатываемый бит окажут воздействие лишь те элементы, которым соответствуют единичное значение битов в индивидуальной окрестности.

ЗАКЛЮЧЕНИЕ

В данной статье рассмотрены основные направления развития теории КА в области защиты информации. Большинство результатов описаны довольно кратко, однако приводятся примеры, иллюстрирующие идею доказательства, а также приводятся ссылки на полные работы, подробно описывающие рассмотренные методы.

В дальнейших исследованиях планируется провести эксперименты с расширением окрестности матрицы КА с набором паттернов и КА с плавающим окном, на основе которых можно будет оценить влияние размера окрестности на степень защищенности информации при ее преобразовании. Также планируется рассмотреть возможность применения функции дополнения последнего сегмента матрицы шифрования («хвоста») для полноты прямоугольного сегмента.

БЛАГОДАРНОСТИ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-31-90069.

СПИСОК ЛИТЕРАТУРЫ

1. *Тоффоли, Т.* Машины клеточных автоматов: Пер. с англ. / Т. Тоффоли, Н. Марголус. – М. : Мир, 1991. – 280 с.

2. *Franti, E.* Cellular Automata Encryption System / E. Franti, M. Dascalu // Proceedings of the Fifth International Conference on Engineering Computational Technology. – Civil-Comp Press, Stirlingshire, UK, 2021. – P. 283–297. DOI: 10.4203 / ccp.84.38.

3. *Khaleel, Gh.* A New Block Cipher Based on Finite Automata Systems / Gh. Khaleel, S. Turaev, T. Mohd, I. Mohd, I. Al-Shaikhli // International Journal on Perceptive and Cognitive Computing. – 2016. – Vol. 2, No 1. DOI: 10.31436/ijpcc.v2i1.31.

4. *Kumaresan, G.* An Analytical Study of Cellular Automata and its Applications in Cryptography / G. Kumaresan, N. Gopalan // International Journal of Computer Network and Information Security. – 2017. – No 12. – P. 45–54. DOI: 10.5815/ijcnis.2017.12.06.

5. *Зотов, Я. А.* Использование клеточных автоматов в симметричной криптосистеме / Я. А. Зотов // Вопросы кибербезопасности. – 2015. – Т. 11, № 3. – С. 43–45.

6. *Taimori, A.* Adaptive Sparse Image Sampling and Recovery / A. Taimori, F. Marvasti // IEEE Transactions on Computational Imaging. – 2018. – Vol. 4, No 3. – P. 311–325. DOI: 10.1109/TCI.2018.2833625.

7. *Hanis, S.* Double image compression and encryption scheme using logistic mapped convolution and cellular automata / S. Hanis, R. Amutha // Multimed Tools Appl. – 2018. – No 77. – P. 6897–6912. DOI: 10.1007/s11042-017-4606-0.

8. *Zhang, F.* Parallel thinning and skeletonization algorithm based on cellular automaton / F. Zhang, X. Chen, X. Zhang // Multimedia Tools

and Applications. – 2020. – No 79. DOI: 10.1007/s11042-020-09660-5.

9. *Roy, S.* IECA: an efficient IoT friendly image encryption technique using programmable cellular automata / S. Roy, U. Rawat, H. A. Sareen, et al. // J Ambient Intell Human Comput. – 2020. – No 11. – P. 5083–5102. DOI: 10.1007 / s12652-020-01813-6.

10. *Ключарёв, П. Г.* Блочные шифры, основанные на обобщённых клеточных автоматах / П. Г. Ключарёв // Наука и образование: электронное научно-техническое издание. – 2012. – № 12. – С. 235–246. DOI: 10.7463/0513.0574231.

11. *Mehta, R. K.* Pattern generation and symmetric key block ciphering using cellular automata / R. K. Mehta, R. Rani // Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI). – Jaipur, India, 2016. – P. 2692–2695. DOI: 10.1109/ICACCI.2016.7732467.

12. *Lira, E.* A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher / E. Lira, H. Macêdo, D. Lima, et al. // Natural Computing. – 2021. – No 2. – P. 1–34.

13. *Achkoun, K.* SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes / K. Achkoun, H. Khadija, C. Hanin, et al. // Journal of Discrete Mathematical Sciences and Cryptography.– 2019. – No 23. – P. 1–16. DOI: 10.1080/09720529.2019.1649031.

14. *Achkoun, K.* SPF-CA-1.2: An enhanced version of cellular automata based block cipher system / K. Achkoun, C. Hanin, A. Sadak, et al. // International Journal of Computer Mathematics: Computer Systems Theory. – 2021. – Vol. 6, No 2. – P. 1–17. DOI: 10.1080/23799927.2021.1942991.

15. *Ключарёв, П. Г.* О производительности блочных шифров, основанных на клеточных автоматах, при их реализации на графических процессорах / П. Г. Ключарёв // Радиооптика. – 2016. – № 6. – С. 24–34. DOI: 10.7463/rdopt.0616.0850899.

16. *Tanasyuk, Y.* Block ciphers on the basis of reversible cellular automata / Y. Tanasyuk, P. Burdeinyi // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska. – 2020. – No 10. – P. 8–11. DOI: 10.35784/iapgos.919.

17. *Kari, J.* Reversibility and surjectivity problems of cellular automata / J. Kari // Journal of Computer and System Science. – 1994. – Vol. 1, No 48. – P. 149–182.

18. *Clarridge, A.* A cryptosystem based on the composition of reversible cellular automata / A. Clarridge, K. Saloma // Proceedings of the International Conference on Language and Automata Theory and Applications. – Springer, Berlin, Heidelberg, 2009. – P. 314–325. DOI: 10.1007/978-3-642-00982-2_27.

19. *Zhu, B.-P.* Public-key cryptosystem based on cellular automata / B.-P. Zhu, L. Zhou, F.-Y. Liu // Journal of NanjingUniversity of Science and Technology. – 2007. – No 31. – P. 612–616.

20. *Sukhinin, B. M.* High-speed pseudorandom sequence generators based on cellular automata / B. M. Sukhinin // Prikl. Diskr. Mat. – 2010. – Vol. 8, No 2. – P. 34–41.

21. *Богаченко, Н. Ф.* Построение генератора псевдослучайных последовательностей на основе клеточного автомата / Н. Ф. Богаченко, И. О. Горохов // Математические структуры и моделирование. – 2020. – Т. 56, № 4. – С. 64–74. DOI: 10.24147/2222-8772.2020.4.64-74

22. *Мухамеджанов, Д. Д.* Генератор псевдослучайных чисел на основе клеточных автоматов / Д. Д. Мухамеджанов, А. Б. Левина // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18, № 5. – С. 894–900. DOI: 10.17586/2226-1494-2018-18-5-894-900.

23. *Ланских, В. Г.* Исследование генераторов псевдослучайных двоичных чисел на основе неоднородных клеточных автоматов с псевдослучайным выбором правил взаимодействия / В. Г. Ланских, Н. А. Титова, Е. В. Кашина, Л. В. Пешнина // ИТ Арктика. – 2018. – № 3. – С. 55–68.

24. *Ключарёв, П. Г.* Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата / П. Г. Ключарёв // Вопросы кибербезопасности. – 2017. – Т. 19, № 1. – С. 45–50. DOI: 10.21581/2311-3456-2017-1-45-50.

25. *Alaa, E. B.* Building Secure and Fast Cryptographic Hash Functions Using Programmable Cellular Automata / E. B. Alaa, M. F. Kamel //

Journal of Computing and Information Technology. – 2015. – No 4. – P. 317–328. DOI:10.2498/cit.1002639.

26. *Rajeshwaran, K.* Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function / K. Rajeshwaran, K. Anil Kumar // Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). – Coimbatore, India, 2019. – P. 1–6. DOI: 10.1109/ICECCT.2019.8869146.

27. *Slimane, N.* Hash Key-Based Image Cryptosystem Using Chaotic Maps and Cellular Automata / N. Slimane, N. Aouf, K. Bouallegue and M. Machhout // Proceedings of the IEEE 15th International Multi-Conference on Systems, Signals & Devices (SSD). – Yasmine Hammamet, Tunisia, 2018. – P. 190–194. DOI: 10.1109/SSD.2018.8570644.

28. *Добрица, В. П.* Последовательные автоматные шифраторы / В. П. Добрица, Д. М. Зарубин, Н. К. Зарубина, А. А. Ноздрина // Известия ЮЗГУ. – 2016. – Т. 18, № 1. – С. 36–39.

29. *Росошек, С. К.* Криптосистемы клеточных автоматов / С. К. Росошек, С. И. Боровков, О. О. Евсютин // Прикладная дискретная математика. – 2008. – № 1. – С. 43–49.

30. *Зарубин, Д. М.* Усовершенствование клеточного автомата с целевой функцией для повышения стойкости / Д. М. Зарубин, В. П. Добрица, Е. В. Шеин // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сб. тр. 1 Всероссийской научно-практической конференции. – Курск, 2017. – С. 227–231.

31. *Добрица, В. П.* Усовершенствование клеточного автомата на разбиении для повышения / В. П. Добрица, М. А. Ефремов, Д. М. Зарубин, А. А. Асютиков // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сб. тр. 1 Всероссийской научно-практической конференции. – Курск, 2017. – С. 224–227.

32. *Асютиков, А. А.* Шифрование клеточным автоматом на разбиении по принципу плавающего окна / В. П. Добрица, А. А. Асютиков // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сб. тр. 2 Всероссийской научно-практической конференции. – Курск, 2018. – С. 45–50.

33. *Kuleshova, E. A.* Multi-threaded data processing system based on cellular automata / E. A. Kuleshova, A. L. Marukhlenko, V. P. Dobritsa, M. O. Tanygin // Proceedings of the 11th Majorov International Conference on Software Engineering and Computer Systems (MICSECS 2019). – Saint Petersburg, 2019. – P. 1–12.

34. *Марухленко, А. Л.* Вариант организации многопоточной обработки конфиденциальных данных на базе клеточных автоматов / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, Д. О. Бобынцев // Известия Юго-Западного государственного университета. – 2019. – Т. 23, № 3. – С. 100–112.

35. *Kuleshova, E. A.* Formation of Unique Characteristics of Hiding and Encoding of Data Blocks Based on the Fragmented Identifier of Information Processed by Cellular Automata / E. A. Kuleshova, A. L. Marukhlenko, V. P. Dobritsa, M. O. Tanygin // Computers 2020. – Vol. 51, No 9. DOI: 10.3390/computers9020051.

Кулешова Елена Александровна — аспирант кафедры информационной безопасности Юго-Западного государственного университета, г. Курск
E-mail: lena.kuleshova.94@mail.ru
ORCID iD: https://orcid.org/0000–0002–8270–564X

DOI: https://doi.org/10.17308/sait.2021.2/3506 ISSN 1995-5499
Received 12.03.2021
Accepted 19.07.2021

APPLICATION OF CELLULAR AUTOMATA IN INFORMATION SECURITY SYSTEMS

© 2021 E. A. Kuleshova✉

Southwest State University
19, building B, Chelyuskintsev Street, 305004 Kursk, Russian Federation

Annotation. The article presents an overview of automatic scramblers based on cellular automata, which are used in information security systems. It considers works on the application of cellular automata in symmetric encryption systems and their practical implementation, as well as the construction of public-key encryption systems based on cellular automata, the use of cellular automata for generating pseudo-random numbers, and methods for the construction of cryptographic hash functions using cellular automata. The article also presents a generalized concept of an abstract automaton and elaborated models of cellular automata, and compares models of cellular automata with an objective function and cellular automata with a floating window, as well as describes their algorithms and evaluates their resistance. In our study, we also considered methods of using cellular automata in multithreaded data processing with the possibility of using patterns that determine the individual neighborhood of the elements during cellular encryption, and the possibility of using a reference book with a set of rules for bypassing the encryption matrix, as well as a method for the one-key transformation of binary data streams with an open parameter based on a cellular automaton with a floating window and a dynamic matrix, divided into elementary segments. The possibility of using cellular automata for multithreaded data processing in real time is considered. In conclusion, the article provides recommendations for enhancing the methods of information protection based on cellular automata, including the method of using an extended key that determines a pseudo-random neighborhood, taking into account the position of the processed bit in the initial data matrix.
Keywords: cellular automaton, sequential automata scrambler, cellular automaton with objective function, cellular automaton with a floating window, block cellular automaton, protection of confidential information, information security, data transformation.

CONFLICT OF INTEREST

The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCES

1. *Toffoli T. & Margolus N.* (1991) Cellular automata machines: Translation from English. Moscow, Mir Publishing.

2. *Franti E. & Dascalu M.* (2021) Cellular Automata Encryption System. In: Topping, B. H. V., Montero, G., Montenegro, R. (eds.) Proceedings of The Fifth International Conference on Engineering Computational Technology. Stirlingshire, Civil-Comp Press. P. 283–297. DOI: 10.4203 / ccp. 84.38.

3. *Khaleel G., Turaev S., Tamrin M. & Al-Shaikhli imad F.* (2016) A New Block Cipher Based on Finite Automata Systems. International Journal on Perceptive and Cognitive Computing. 2 (1). doi: 10.31436 / ijpcc.v2i1.31.

4. *Kumaresan G. & Gopalan N.* (2017) An Analytical Study of Cellular Automata and its Applications in Cryptography. International Journal of Computer Network and Information Security. 12. P. 45–54. DOI: 10.5815 / ijcnis.2017.12.06.

5. *Zotov Ya. A.* (2015) The use of cellular automata in a symmetric cryptosystem. Cybersecurity Issues. 3 (11). P. 43–45.

6. *Taimori A. & Marvasti F.* (2018) Adaptive Sparse Image Sampling and Recovery. IEEE

✉ Kuleshova Elena A.
e-mail: lena.kuleshova.94@mail.ru

Transactions on Computational Imaging. 4 (3). P. 311–325. DOI: 10.1109 / TCI.2018.2833625.

7. *Hanis S. & Amutha R.* (2018) Double image compression and encryption scheme using logistic mapped convolution and cellular automata. Multimed Tools Appl. 77, P. 6897–6912. DOI: 10.1007 / s11042-017-4606-0.

8. *Zhang F., Chen X. & Zhang X.* (2020) Parallel thinning and skeletonization algorithm based on cellular automaton. Multimedia Tools and Applications. 79 (12). DOI: 10.1007 / s11042-020-09660-5.

9. *Roy S., Rawat U., Sareen H. & Nayak S.* (2020) IECA: an efficient IoT friendly image encryption technique using programmable cellular automata. J Ambient Intell Human Comput. 11. P. 5083–5102. DOI: 10.1007 / s12652-020-01813-6.

10. *Klyucharyov P. G.* (2012) Block ciphers based on generalized cellular automata. Science and education: electronic scientific and technical publication. 12. P. 235–246. DOI: 10.7463 / 0513.0574231.

11. *Mehta R. K. & Rani R.* (2016) Pattern generation and symmetric key block ciphering using cellular automata. Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI 2016), Jaipur, India. P. 2692–2695. DOI: 10.1109 / ICACCI.2016.7732467.

12. *Lira E., Macêdo H., Lima D., Alt L. & Oliveira G.* (2021). A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher. Natural Computing. 2. P. 1–34.

13. *Achkoun, K., Hanin, C. & Omary, F.* (2019) SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes. Journal of Discrete Mathematical Sciences and Cryptography. 23. P. 1–16. DOI: 10.1080/09720529.2019.1649031.

14. *Achkoun K., Hanin C., Sadak A., Ziani F. E. & Omary F.* (2021) SPF-CA-1.2: An enhanced version of cellular automata based block cipher system. International Journal of Computer Mathematics: Computer Systems Theory. 6 (2). P. 1–17. DOI: 10.1080/23799927.2021.1942991.

15. *Klyucharyov P. G.* (2016) On the performance of block ciphers based on cellular automata when they are implemented on graphic processors. J. Radio optics. 6. P. 24–34. DOI: 10.7463 / rdopt.0616.0850899.

16. *Tanasyuk Y. & Burdeinyi P.* (2020) Block ciphers on the basis of reversible cellular automata. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska. 10. P. 8–11. DOI: 10.35784 / iapgos.919.

17. *Kari J.* (1994) Reversibility and surjectivity problems of cellular automata. Journal of Computer and System Science. 1 (48). P. 149–182.

18. *Clarridge A. & Salomaa K.* (2009) A Cryptosystem Based on the Composition of Reversible Cellular Automata. In: Dediu, A. H., Ionescu, A. M., Martín-Vide, C. (eds.) Language and Automata Theory and Applications, LATA 2009. LNCS, vol 5457. Springer, Berlin, Heidelberg. P. 314–325. DOI: 10.1007/978-3-642-00982-2_27.

19. *Zhu B.-P., Zhou L. & Liu F.-Y.* (2007) Public-key cryptosystem based on cellular automata. Journal of Nanjing University of Science and Technology. 31. P. 612–616.

20. *Sukhinin B. M.* (2010) High-speed pseudorandom sequence generators based on cellular automata. Prikl. Diskr. Mat. 8 (2). P. 34–41.

21. *Bogachenko N. F. & Gorokhov I. O.* (2020) Construction of a pseudo-random sequence generator based on a cellular automaton. Mathematical structures and modeling. 4 (56). P. 64–74. DOI: 10.24147 / 2222-8772.2020.4.64-74.

22. *Mukhamedzhanov D. D. & Levin A. B.* (2018) Pseudo-random number generator based on cellular automata. Scientific and technical bulletin of information technologies, mechanics and optics. 5 (18). P. 894–900. DOI: 10.17586/2226-1494-2018-18-5-894-900.

23. *Lanskikh V. G., Titova N. A., Kashina E. V. & Peshnina L. V.* (2018) Investigation of generators of pseudo-random binary numbers based on inhomogeneous cellular automata with a pseudo-random choice of interaction rules. J. IT Arctic. 3. P. 55–68.

24. *Klyucharyov P. G.* (2017) Method for constructing cryptographic hash functions based on iterations of a generalized cellular automaton. Cybersecurity Issues. 1 (19). P. 45–50. DOI: 10.21581 / 2311-3456-2017-1-45-50.

25. *Alaa E. B. & Kamel M. F.* (2015) Building Secure and Fast Cryptographic Hash Functions Using Programmable Cellular Automata. Journal

of Computing and Information Technology. 4. P. 317–328. DOI: 10.2498 / cit. 1002639.

26. *Rajeshwaran K. & Anil Kumar K.* (2019) Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function. Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT 2019), Coimbatore, India. P. 1–6. DOI: 10.1109 / ICECCT.2019.8869146.

27. *Slimane N., Aouf N., Bouallegue K. & Machhout M.* (2018) Hash Key-Based Image Cryptosystem Using Chaotic Maps and Cellular Automata. Proceedings of the IEEE 15th International Multi-Conference on Systems, Signals & Devices (SSD), Yasmine Hammamet, Tunisia. P. 190–194. DOI: 10.1109 / SSD.2018.8570644.

28. *Dobritsa V. P., Zarubin D. M., Zarubina N. K. & Nozdrina A. A.* (2016) Sequential automatic encoders. Bulletin of the Southwest State University. 1 (18). P. 36–39.

29. *Rososhek S. K., Borovkov S. I. & Evsyutin O. O.* Cryptosystems of cellular automata. Applied discrete mathematics. 1. P. 43–49.

30. *Zarubin D. M., Dobritsa V. P. & Shein E. V.* (2017) Improvement of a cellular automaton with a target function to increase resistance. In: Andronov, V. G. (eds.) 1st All-Russian Scientific and Practical Conference: Proceedings of the Infocommunications and space technologies: state, problems and solutions, Kursk, Russia. P. 227–231.

31. *Dobritsa V. P., Efremov M. A., Zarubin D. M. & Asyutikov A. A.* (2017) Improvement of a cellular automaton on a partition for increasing. In: Andronov, V. G. (eds.) 1st All-Russian Scientific and Practical Conference: Proceedings of the Infocommunications and space technologies: state, problems and solutions, Kursk, Russia. P. 224–227.

32. *Asutikov A. A. & Dobritsa V. P.* (2018) Encryption by a cellular automaton on a partition according to the floating window principle. In: Andronov, V. G. (eds.) 2nd All-Russian Scientific and Practical Conference: Proceedings of the Infocommunications and space technologies: state, problems and solutions, Kursk, Russia. P. 45–50.

33. *Kuleshova E. A., Marukhlenko A. L., Dobritsa V. P. & Tanygin M. O.* (2019) Multi-threaded data processing system based on cellular automata. Proceedings of the 11th Majorov International Conference on Software Engineering and Computer Systems (MICSECS 2019), Saint Petersburg. P. 1–12.

34. *Marukhlenko A. L., Plugatarev A. V., Tanygin M. O., Marukhlenko L. O. & Bobintsev D. O.* (2019) Variant of organizing multithreaded processing of confidential data based on cellular automata. Bulletin of the Southwest State University. 3 (23). P. 100–112.

35. *Kuleshova E. A., Marukhlenko A. L., Dobritsa V. P. & Tanygin M. O.* (2020) Formation of Unique Characteristics of Hiding and Encoding of Data Blocks Based on the Fragmented Identifier of Information Processed by Cellular Automata. Computers. 9 (51). DOI: 10.3390 / computers9020051.

Kuleshova Elena A. — postgraduate student, Department of Information Security, Southwest State University, Kursk.
E-mail: lena.kuleshova.94@mail.ru
ORCID iD: https://orcid.org/0000–0002–8270–564X