КЛЕТОЧНЫЕ АВТОМАТЫ И ИХ ОБОБЩЕНИЯ В ЗАДАЧАХ КРИПТОГРАФИИ. ЧАСТЬ 2

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 была посвящена классическим клеточным автоматам и основанным на них симметричным криптографическим алгоритмам. В ней кратко обсуждалась история развития теории клеточных автоматов и ее применения в различных научных областях. Был 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 был дан обзор статей, посвященных использованию двухмерных клеточных автоматов для построения симметричных криптоалгоритмов (этот подход давал лучшие результаты). Также были упомянуты многомерные клеточные автоматы. Настоящая вторая часть статьи содержит обзор 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, уделено внимание интересным связям обобщенных клеточных автоматов, в контексте их использования в криптографии, с теорией расширяющих графов; также уделено внимание вопросам стойкости криптоалгоритмов, основанных на обобщенных клеточных автоматах. Упомянуты работы, посвященные реализации различных криптографических алгоритмов, основанных на обобщенных клеточных автоматах, на программируемых логических интегральных схемах и графических процессорах. Дан обзор асимметричных криптоалгоритмов, основанных на клеточных автоматах. 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: *Клеточный автомат, обобщенный клеточный автомат поточный шифр, блочный шифр, хэш-функция, граф Рамануджана, асимметричный криптоалгоритм.*

DOI:10.21681/2311-3456-2022-1-37-48

Введение

Первая части статьи была посвящена обзору литературы, связанной с использованием клеточных автоматов в симметричной криптографии. В частности, в первой части кратко обсуждалась история развития теории клеточных автоматов и были рассмотрены симметричные криптоалгоритмы, основанные на клеточных автоматах (в основном – одномерных и двухмерных).

Настоящая вторая часть статьи посвящена главным образом обзору литературы, связанной с использованием в криптографии обобщенных клеточных автоматов. С помощью таких автоматов можно производить построение рассчитанных на аппаратную реализацию высокопроизводительных симметричных криптографических алгоритмов, в том числе, алгоритмов поточного шифрования, алгоритмов блочного шифрования и криптографических хэш-функций. В частности, речь идет о построении обобщенных клеточных автоматов и основанных на них криптоалгоритмов, о результатах анализа криптостойкости таких алгоритмов, о производительности их реализаций. Затрагиваются также вопросы построения графов, лежащих в основе обобщенных клеточных автоматов. Кроме того, дан обзор асимметричных криптоалгоритмов, основанных на клеточных автоматах. Также рассмотрен ряд теоретико-сложностных результатов, связанных с клеточными автоматами.

1. Обобщенные клеточные автоматы в симметричной криптографии

1.1 Основные понятия

Развитие применения клеточных автоматов в симметричной криптографии оказалось связанным с обобщенными клеточными автоматами. Прежде чем дать определение таким автоматам, отметим, что в

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

данной работе мы будем использовать термин «граф», допуская наличие петель и кратных ребер.

Итак, назовем обобщенным клеточным автоматом ориентированный граф (граф обобщенного клеточного автомата) с множеством вершин $V = \{v_1, \ldots, v_N\}$, с каждой вершиной v_i которого ассоциированы:

- булева переменная m_i, которая называется ячейкой;
- булева функция $f_i(x_1, \ldots, x_{d_i})$, которая называется локальной функцией связи вершины v_i (d_i – степень захода вершины v_i).

При этом каждой паре (v, e), где $v \in V$ – вершина, e – входящее в нее ребро, соответствует номер аргумента локальной функции связи, вычисляемой в вершине v. Будем называть его номером ребра e относительно вершины v.

Опишем теперь работу обобщенного клеточного автомата. В начальный момент времени каждая ячейка m_i, $i = 1 \ldots N$, имеет некоторое начальное значение $m_i(0)$. Автомат работает пошагово. Значения ячеек на шаге номер t вычисляются по формуле:

$$m_i(t) = f_i(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \ldots, m_{\eta(i,d_i)}(t-1)), \quad (1)$$

где $\eta(i, j)$ – номер вершины, из которой выходит ребро, входящее в вершину v_i и имеющее относительно этой вершины номер j.

Очевидно, что определенный таким образом обобщенный клеточный автомат является автономным конечным автоматом.

Заполнением обобщенного клеточного автомата $M(t)$ на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \ldots, m_N(t))$.

Обобщенный клеточный автомат будем называть однородным, если для любого $i \in \{1, \ldots, N\}$ выполняется $f_i = f$, то есть локальная функция связи для всех ячеек одинакова. Степени захода вершин графа однородного обобщенного клеточного автомата, очевидно, одинаковы: $d_1 = d_2 = \ldots = d_N = d$. Обобщенный клеточный автомат, не являющийся однородным, будем называть неоднородным.

Назовем обобщенный клеточный автомат неориентированным, если для любого ребра (u, v) в его графе существует и ребро (v, u). Граф такого автомата можно рассматривать как неориентированный, для чего достаточно заменить каждую пару ориентированных ребер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$.

Здесь мы будем в основном иметь дело с неориентированными однородными обобщенными клеточными автоматами. Такой автомат задается тройкой (G, f, η), где G – d-регулярный граф обобщенного клеточного автомата (множество его вершин $V = \{v_1, \ldots, v_N\}$), а $\eta : \{1, \ldots, N\} \times \{1, \ldots, d\} \to \{1, \ldots, N\}$ – введенная выше функция (будем называть ее функцией нумерации ребер).

Некоторый набор ячеек обобщенного клеточного автомата будем называть выходом. Выходной последовательностью клеточного автомата A назовем функцию $F_A : \{0,1\}^N \times \mathbb{N} \to \{0,1\}^m$, аргументами которой является начальное заполнение обобщенного клеточного автомата и номер шага, а значением – значение выхода на этом шаге (здесь m – длина выхода). Периодом клеточного автомата будем называть период последовательности его заполнений.

1.2 История развития обобщенных клеточных автоматов

Фактически, обобщения понятия клеточного автомата, подобные введенному выше, независимо предлагались разными авторами и применялись в различных областях. По-видимому, впервые подобное понятие появилось в 1969 г. в работе [1], где такие автоматы использовались в области биологии. После этого, в исследовании подобных моделей наступил перерыв, который закончился лишь после 2000 года, когда появился ряд работ, в которых их исследования продолжились. Называли такие автоматы в этих статьях по-разному, например, булевыми сетями (Boolean networks), сетями Кауфмана, графовыми клеточными автоматами и др. (отношение к таким моделям как к обобщению клеточных автоматов более характерно для российской научной школы). В работах [2, 3] рассматривались вероятностные варианты подобных моделей. Кроме того, такие модели исследовались с точки зрения теории динамических систем в работах [4–7] (в частности, изучались вопросы, связанные с числом аттракторов).

С точки зрения теории сложности булевых функций, обобщенные клеточные автоматы рассматривались в работе [8], где доказывается теорема о том, что булеву функцию $\varphi(x_1, \ldots, x_n)$, имеющую при реализации булевой схемой над базисом B сложность l и глубину h, можно вычислить с помощью обобщенного клеточного автомата, локальные функции связи которого принадлежат B, а граф имеет $n + l$ вершин, причем для этого требуется не более h шагов. Эта теорема, устанавливая связь между обобщенными клеточными автоматами и схемами из функциональных элементов, показывает универсальность обобщенных клеточных автоматов, как вычислительной модели. Фактически, такие автоматы можно рассматривать как вычислительную модель параллельной обработки информации.

1.3 Применение обобщенных клеточных автоматов в симметричной криптографии

Использовать обобщенные клеточные автоматы в симметричной криптографии впервые предложил Б.М. Сухинин в 2009 – 2011 гг. в работах [9,10] и др., в которых он называл аналогичную модель неоднородным клеточным автоматом (мы этот термин используем в другом значении). В его работах под этим термином понимается автономный конечный автомат, состояние которого задается совокупностью из N ячеек, значение каждой из которых обновляется на каждом шаге исходя из значений некоторой ее окрестности на предыдущем шаге с помощью булевой функции, называемой локальной функцией связи. Причем окрестность ячейки – это некоторый на-

бор ячеек, свой для каждой ячейки. Входящие в него ячейки могут быть выбраны произвольным образом из всей совокупности ячеек такого автомата так, чтобы окрестность каждой ячейки содержала одинаковое число ячеек. В диссертации [9] приведено строгое определение такого автомата. Там же на основе таких автоматов, выбранных методом рандомизированного перебора, построен генератор псевдослучайных последовательностей, в соответствии со схемой, приведенной на рис. 1 (Б.М. Сухининым было предложено два генератора на базе этой схемы: один – на основе двухмерных клеточных автоматов, а другой – на основе обобщенных клеточных автоматов). Такие генераторы показали высокую скорость работы при аппаратной реализации (на ПЛИС).

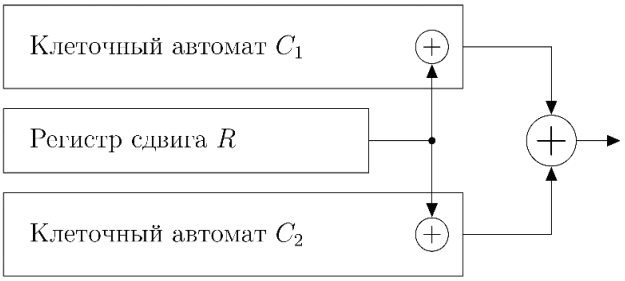

Рис. 1: Структура генератора псевдослучайных последовательностей, предложенная в работе [9]

После вышеупомянутых работ стало ясно, что симметричные криптоалгоритмы, основанные на обобщенных клеточных автоматах, являются весьма перспективными. Появились следующие естественные вопросы:

- Можно ли на основе обобщенных клеточных автоматов построить не только поточные шифры, но и блочные шифры, а также криптографические хэш-функции?
- Как правильно выбирать граф, локальную функцию связи и другие параметры обобщенного клеточного автомата, предназначенного для использования в составе симметричных криптографических алгоритмов? Можно ли это делать исходя из теоретических соображений, а не перебором?

Эти вопросы, как и ряд других, подробно исследованы в работах автора настоящей статьи. В частности, оказалось, что граф должен удовлетворять ряду свойств, а именно, он должен быть регулярным, не должен быть двудольным, должен иметь возможно меньшее число кратных ребер и как можно меньшую, но не меньшую четырех, степень. Этим требованиям удовлетворяют некоторые расширяющие графы, в особенности, некоторые семейства так называемых графов Рамануджана, являющихся, в определенном смысле, асимптотически наилучшими расширяющими графами.

В работах [8,11,12] исследованы свойства, которым должны удовлетворять граф, локальная функция связи и функция нумерации ребер обобщенного клеточного автомата. Обосновано, что локальная функция связи должна быть равновесной, шефферовой и как можно более нелинейной, но линейно зависящей от одного из своих аргументов (напомним, что нелинейностью булевой функции называется расстояние Хемминга от нее до множества аффинных булевых функций). Построено семейство локальных функций связи, удовлетворяющих этим требованиям. Введено понятие t-шаговой коллизии веса w, представляющей собой такие два различных заполнения $x_1, x_2 \in \{0,1\}^N$ обобщенного клеточного автомата CA, что $|x_1 \oplus x_2| = w$ и $CA(t, x_1) = CA(t, x_2)$, но $CA(t-1, x_1) \neq CA(t-1, x_2)$, где $|x|$ – вес вектора x, $CA(t, x)$ – заполнение на шаге t обобщенного клеточного автомата CA с начальным заполнением x. Доказано, что для обеспечения устойчивости однородных неориентированных обобщенных клеточных автоматов к одношаговым коллизиям веса 1 достаточно, чтобы локальная функция связи линейно зависела от одного из своих аргументов, а соответствующие этим аргументам ребра графа обобщенного клеточного автомата порождали 2-фактор.

В работе [13] на основе общей схемы (рис. 1), предложенной ранее в [9], построен поточный шифр, представляющий собой генератор гаммы, состоящий из двух различных неориентированных однородных обобщенных клеточных автоматов (CA_1, CA_2), к одной из ячеек (задающей ячейке) каждого из которых прибавляется по модулю 2 очередной разряд последовательности, порождаемой линейным регистром сдвига с обратной связью. При этом, в качестве графов этих автоматов взяты графы Рамануджана, в качестве локальных функций связи – различные функции из специально построенного семейства, а задающая ячейка выбрана из ряда теоретических соображений. На каждом шаге с каждого автомата снимаются значения определенного набора ячеек, и поразрядная сумма по модулю 2 полученных двух наборов значений подается на выход генератора гаммы. Начальным заполнением каждого обобщенного клеточного автомата является ключ *key*, конкатенированный с некоторой константой, дополняющей его до размера автомата. На основе ключа также вырабатывается начальное заполнение линейного регистра сдвига с обратной связью.

Обозначим заполнение обобщенного клеточного автомата CA с задающей ячейкой на шаге t, как $CA(t, M_0, \xi)$, где M_0 – начальное заполнение, а ξ – подаваемая на задающую ячейку последовательность. Выход обобщенного клеточного автомата обозначим $pr_m(CA(t, M_0, \xi))$, где m – длина выхода, а pr_m – функция, возвращающая некоторые m разрядов аргумента (имеющие наперед заданные номера). Последовательность ξ вырабатывается линейным регистром сдвига с обратной связью, начальное заполнение которого получено на основе ключа *key*. Выход генератора гаммы на шаге t вычисляется по формуле:

$$y(key, t) = \\ = pr_m(CA_1(t, key \,||\, c_1, \xi)) \oplus pr_m(CA_2(t, key \,||\, c_2, \xi)), \quad (2)$$

где c_1 и c_2 – константы, дополняющие ключ до размера обобщенного клеточного автомата, вес которых должен быть близок к половине длины; || – операция конкатенации.

Вырабатываемая генератором гамма представляет собой конкатенацию выходов, после определенного числа (τ) холостых шагов: $\gamma = y(key,\tau+1) \| y(key,\tau+2) \| \ldots$.

Кроме того, в работе [13] понятие пространственной характеристики лавинного эффекта обобщено на обобщенные клеточные автоматы.

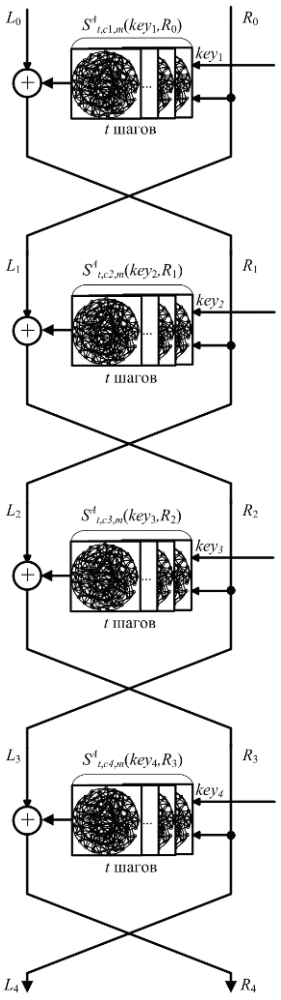

Рис. 2: Общая схема алгоритма блочного шифрования, основанного на обобщенных клеточных автоматах

В работе [14] предложена конструкция псевдослучайных функций-кандидатов (т.е., неформально говоря, функций, которые нельзя отличить от случайных с помощью специального набора тестов), основанная на обобщенных клеточных автоматах. Аргумент функции, ключ и специальная константа подаются на обобщенный клеточный автомат (в качестве начального заполнения). Он совершает определенное число шагов, после чего результат снимается с определенного набора ячеек. Автомат синтезируется исходя из ряда теоретических соображений (в частности, в качестве графа используется тот или иной граф Рамануджана, а о выборе локальной функции связи сказано выше). На базе таких псевдослучайных функций-кандидатов предложено семейство блочных шифров [15]. Такие шифры (рис. 2) используют схему Фейстеля с небольшим числом раундов. В качестве раундовой функции используется псевдослучайная функция-кандидат. При этом, она используется, в том числе, и для смешивания подблока с ключом, что существенно затрудняет применение разностного криптоанализа к таким шифрам.

В работе [16] предложено использовать в аналогичных блочных шифрах вместо классической схемы Фейстеля обобщенную (в которой блок разделяется больше, чем на две части). В этом случае, можно использовать обобщенный клеточный автомат с меньшим числом ячеек, что приводит к меньшему объему вычислений на каждом шаге. Вместе с тем это, по-видимому, приведет к необходимости в увеличении числа раундов, так что влияние применения обобщенной схемы Фейстеля на быстродействие является спорным и требующим дополнительных исследований.

Кроме того, на обобщенных клеточных автоматах основаны два семейства криптографических хэш-функций: на основе древовидной схемы [17] и на основе конструкции, похожей на криптографическую губку [18], а также семейство алгоритмов выработки имитовставок [19].

1.4 Обобщенные клеточные автоматы и расширяющие графы

Как уже говорилось, в качестве графов обобщенных клеточных автоматов хорошо подходят расширяющие графы [20], в особенности, так называемые графы Рамануджана, которые являются в определенном смысле асимптотически наилучшими расширяющими графами.

Напомним, что коэффициентом реберного расширения неориентированного d-регулярного графа G с множеством вершин V называется величина $h(G) = \min\limits_{S \subset V : 0 < |S| \le \frac{|V|}{2}} \frac{|\partial S|}{|S|}$, где $|\partial S|$ – число ребер, каждое из которых соединяет вершину из множества S с вершиной из множества $V \setminus S$. Расширяющим графом (expander graph) называется неориентированный регулярный граф G, для которого $h(G) \ge c$, где c – некоторая наперед заданная положительная константа. Коэффициент реберного расширения неориентированного графа связан с его спектром (т.е. набором собственных значений его матрицы смежности, отсортированным по невозрастанию: $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_N$). Известно, что для d-регулярных графов $\lambda_1 = d$ и справедливо следующее соотношение (неравенство Чигера): $\frac{1}{2}(d-\lambda_2) \le h(G) \le \sqrt{2d(d-\lambda_2)}$. Введем обозначение: $\lambda = \lambda(G) = \max_{|\lambda_i|<d} |\lambda_i|$.

Для диаметра расширяющего графа имеет место неравенство: $D \leqslant \left\lceil \log_{d/|\lambda_2|}(N-1) \right\rceil$. Оно является одним из аргументов в пользу того, что в качестве графов неориентированных обобщенных клеточных автоматов хорошо подходят графы с маленьким значением параметра λ_2 (этот вопрос рассматривается, в частности, в работе [21]). Такими графами являются графы Рамануджана (т.е. связные *d*-регулярные графы, для которых выполняется неравенство $\lambda(G) \le 2\sqrt{d-1}$). Для диаметра $D(G)$ графов Рамануджана известна верхняя оценка $D(G) \le 2\log_{d-1} N + \mathrm{O}(1)$, которая близка к нижней оценке диаметра регулярного графа. В работе [13] впервые предложено использовать такие графы в качестве графов обобщенных клеточных автоматов, предназначенных для криптографических применений. Маленький диаметр таких графов приводит к тому, что число шагов, за которое у основанных на таких графах обобщенных клеточных автоматов обеспечивается зависимость значений всех ячеек от начального значения каждой ячейки, при правильном выборе локальной функции связи составляет порядка $O(\log N)$. Такой же порядок имеет число шагов, необходимое для достижения оптимальных значений интегральной и пространственной характеристик лавинного эффекта у этих автоматов. Это существенно лучше, по сравнению с классическими клеточными автоматами.

В работе [22] изучается рандомизированный метод построения графов Рамануджана, подходящих для обобщенных клеточных автоматов. А в работе [21] изучаются графы Рамануджана, которые строятся с помощью детерминированных методов. В ней с целью выбора графов, подходящих для построения обобщенных клеточных автоматов, рассмотрены четыре семейства графов Рамануджана: семейства X и Y Любоцкого–Филипса–Сарнака, семество Пайзера и семейство Моргенштерна. Из них для обобщенных клеточных автоматов подходят семейство графов Пайзера [23–25] (их также называют графами изогений суперсингулярных эллиптических кривых [26,27]) и семейство Y графов Любоцкого–Филипса–Сарнака (LPS-Y) [28].

Графы Пайзера устроены следующим образом. Множеством вершин графа является множество классов изоморфизма суперсингулярных эллиптических кривых над полем $\mathbb{F}_{p^2}$. Две вершины графа Пайзера соединены ребром тогда и только тогда, когда между представителями соответствующих им классов изоморфизма существует l-изогения (напомним, что l-изогенией из эллиптической кривой E_1 в эллиптическую кривую E_2 называется морфизм $\psi : E_1 \to E_2$, такой что $\psi(O) = O$, и имеющий мощность ядра в алгебраическом замыкании базового поля, равную l). Такой граф является недвудольным $(l+1)$-регулярным графом Рамануджана. Интересно, что графы изогений суперсингулярных эллиптических кривых находят применение в постквантовой криптографии – на них основан постквантовый протокол выработки общего ключа SIDH [29] и базирующийся на нем протокол Форзиция [30].

Графы LPS-Y строятся следующим образом. Выбираются простые числа p и q, для которых выполняется: $p \equiv 1 \pmod 4$; $q \equiv 1 \pmod 4$; $p \ne q$; $\left(\frac{p}{q}\right) = 1$, где $\left(\frac{p}{q}\right)$ – символ Лежандра. Множеством V вершин этого графа является проективная прямая над конечным полем $\mathbb{F}_q$, т.е., $V = \mathbb{F}_q \bigcup \{\infty\}$. Каждая вершина $u \in V$ соединена ребром с вершиной v, такой что:

$$v = \begin{cases} \dfrac{(a_0 + ia_1)u + (a_2 + ia_3)}{(-a_2 + ia_3)u + (a_0 - ia_1)}, \\ \text{если } (a_2 - ia_3)u \ne (a_0 - ia_1) \text{ и } u \ne \infty, \\ \infty, \text{ если } (a_2 - ia_3)u = (a_0 - ia_1) \text{ и } u \ne \infty, \\ \dfrac{ia_1 + a_0}{ia_3 - a_2}, \text{ если } ia_3 \ne a_2 \text{ и } u = \infty, \\ \infty, \text{ если } ia_3 = a_2 \text{ и } u = \infty, \end{cases} \qquad (3)$$

для каждой четверки $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, такой, что a_0 – нечетное положительное, a_1, a_2, a_3 – четные и выполняется равенство: $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. Здесь $i \in \mathbb{F}_q$ такое, что $i^2 + 1 = 0$. Такие графы являются $(p+1)$-регулярными графами Рамануджана [28].

1.5 О криптоанализе симметричных криптографических алгоритмов, основанных на обобщенных клеточных автоматах

Различные аспекты стойкости криптографических алгоритмов, основанных на обобщенных клеточных автоматах, исследуются в ряде работ. Так, в работе [31] получены условия стойкости рассматриваемых алгоритмов блочного шифрования по отношению к линейному криптоанализу. Соображения, связанные с квантовым криптоанализом рассматриваемых криптоалгоритмов, приведены в работе [32]. В ряде работ приведены экспериментальные исследования криптостойкости основанных на обобщенных клеточных автоматах криптоалгоритмов по отношению к различным методам криптоанализа. В частности, в работе [33] приведены результаты экспериментов, связанных с алгебраическим криптоанализом. Решается система полиномиальных уравнений, описывающая преобразование, выполняемое обобщенным клеточным автоматом, посредством построения базиса Гребнера, для чего используется алгоритм Фужера F4, реализованный в библиотеке Polybori и в системе компьютерной алгебры Magma. Оказывается, что при правильном выборе параметров обобщенного клеточного автомата, такую систему можно решить лишь

для совсем маленьких автоматов, состоящих из не более чем двух десятков ячеек (на практике используются обобщенные клеточные автоматы из сотен, а то и тысяч ячеек). В работе [34] эмпирически исследуется применимость логического метода криптоанализа к обобщенным клеточным автоматам – строится конъюнктивная нормальная форма, описывающая преобразование, выполняемое обобщенным клеточным автоматом, и производится решение задачи КНФ-выполнимости посредством SAT-решателей. Снова оказалось, что при правильно выбранных параметрах, на практике можно решить эту задачу лишь для очень маленьких обобщенных клеточных автоматов, причем за время существенно (на несколько порядков) большее, чем полный перебор.

В целом, существующие работы убедительно продемонстрировали стойкость основанных на обобщенных клеточных автоматах симметричных криптографических алгоритмов по отношению к целому ряду методов криптоанализа. Хотя очевидно, что исследования криптостойкости таких алгоритмов следует продолжать.

1.6 О реализации симметричных криптографических алгоритмов, основанных на обобщенных клеточных автоматах, для различных платформ

Производительности и эффективности реализации рассматриваемых криптоалгоритмов на программируемых логических интегральных схемах (ПЛИС) посвящены работы [35,36], согласно которым такие криптографические алгоритмы являются очень эффективными при аппаратной реализации. Так, производительность поточного шифра, основанного на обобщенных клеточных автоматах, при определенных параметрах, на ПЛИС Altera Stratix V, превышает 1100 Гбит/с, что в десятки раз выше производительности традиционных поточных шифров, ориентированных на аппаратную реализацию (таких, как Trivium [37]). Кроме того, такие шифры могут быть реализованы на системах с ограниченными ресурсами (от 1 тыс. LE).

Криптографические алгоритмы, основанные на обобщенных клеточных автоматах, рассчитаны, в первую очередь, на аппаратную реализацию. В то же время, при программной реализации на обычных CPU их производительность невелика. Заметим, что это является не недостатком таких криптоалгоритмов, а особенностью их сферы применимости. Вместе с тем, тот факт, что обобщенный клеточный автомат состоит из набора ячеек, над которыми производятся однотипные вычисления, позволяет добиться эффективной реализации на современных графических процессорах. Реализации криптографических алгоритмов, основанных на обобщенных клеточных автоматах, для графических процессоров посвящены работы [38–40]. В них достигнута производительность в сотни Мбит/с. Учитывая, что графические процессоры присутствуют в большинстве современных персональных компьютеров, а также в смартфонах, планшетах и др., этот факт существенно расширяет область применимости таких шифров.

2. Асимметричные криптосистемы на основе клеточных автоматов

В настоящее время асимметричная криптография (криптография с открытым ключом) переживает своеобразный кризис – наиболее часто используемые асимметричные криптографические алгоритмы и протоколы, основанные на высокой вычислительной сложности задач факторизации целых чисел или дискретного логарифмирования (в частности, алгоритмы RSA и Эль-Гамаля, протокол Диффи-Хеллмана и др.), окажутся нестойкими в случае появления практических образцов квантовых компьютеров, на которых эти задачи решаются за полиномиальное время с помощью квантовых алгоритмов Шора. Поэтому сейчас развивается постквантовая криптография – дисциплина, изучающая асимметричные криптографические алгоритмы, для которых неизвестны эффективные, работающие на квантовом компьютере, методы криптоанализа.

На основе клеточных автоматов наиболее известны две довольно похожие асимметричные криптосистемы: криптосистема Дж. Кари и криптосистема П. Гуаня. Обе они основаны на идее построения конечно-автоматной асимметричной криптосистемы FAPKC (Finite Automaton Public Key Cryptosystems). Эта криптосистема была предложена в работе [41], ей также посвящена работа [42]. В криптосистеме FAPKC закрытый ключ состоит из двух обратимых конечных автоматов, а открытый ключ представляет собой их композицию, которую, вообще говоря, сложно обратить. Было предложено достаточно много вариантов этой криптостистемы. Некоторые из них были взломаны (см., например, работы [43,44]), однако каких-либо фундаментальных уязвимостей этого подхода неизвестно.

Криптосистема, предложенная Дж. Кари в работе [45], основана на доказанной им теореме о том, что задача определения обратимости двухмерного клеточного автомата с бесконечным множеством ячеек является алгоритмически неразрешимой. В этой криптосистеме берется конечная последовательность заведомо обратимых клеточных автоматов специального вида (так называемых маркеров) $C_1 \dots C_n$, клеточные автоматы, обратные к которым, известны. Если эта последовательность известна, то по ней можно вычислить как композицию этих клеточных автоматов:

$$C = C_n \circ C_{n-1} \circ \dots \circ C_1, \quad (4)$$

так и клеточный автомат, обратный к ней:

$$C^{-1} = C_1^{-1} \circ C_2^{-1} \circ \dots \circ C_n^{-1}, \quad (5)$$

Однако если эта последовательность неизвестна, а известен только клеточный автомат C, то задача его обращения, по-видимому, является вычислительно сложной.

В этой криптосистеме закрытым ключом является последовательность клеточных автоматов специального вида $C_1 \dots C_n$, а открытым ключом – их композиция C. Шифрование осуществляется следующим образом: сообщение размещается в ячейках клеточного

автомата C, осуществляется некоторое фиксированное число шагов этого автомата, после чего состояние клеточного автомата C трактуется как шифртекст. Расшифрование осуществляется аналогично – с помощью клеточного автомата C^{-1}, который вычисляется по закрытому ключу. При этом клеточные автоматы должны быть k-мерными, где $k \geqslant 2$.

Безопасность этой криптосистемы рассматривается, в частности, в статье [46] и в диссертации [47].

Более ранняя криптосистема, предложенная П. Гуанем в работе [48], тоже основана на трудности обращения клеточного автомата. Закрытым ключом в ней являются два легко обратимых клеточных автомата, а открытым ключом – их композиция. В остальном данная криптосистема аналогична криптосистеме Кари. На подобном принципе (композиции легко обратимых клеточных автоматов) построена и менее известная криптосистема, предложенная в работе [49].

В подобных криптосистемах проблемным является вопрос построения обратимых клеточных автоматов. Возможно, новые подходы к решению этой задачи, например, развиваемые в работах [50,51] методы, будут способствовать построению новых асимметричных криптосистем. В целом представляется, что все еще остающиеся плохо исследованными асимметричные криптосистемы, основанные на клеточных автоматах, могут представлять интерес с точки зрения использования в асимметричной криптографии, в том числе, в постквантовой.

3. Клеточные автоматы и теория сложности алгоритмов

Вопросы, связанные с вычислительной сложностью некоторых задач на клеточных автоматах, очень важны для обоснования стойкости основанных на них криптоалгоритмов. В частности, с этой точки зрения интересны результаты о NP-полноте. Класс NP-полных задач занимает важнейшее место в теории алгоритмов [52]. Принадлежность распознавательного аналога задачи к классу NP-полных задач говорит о ее высокой вычислительной сложности (в естественном и широко принятом предположении, что $\mathrm{P} \neq \mathrm{NP}$). Также могут быть интересны результаты о принадлежности некоторых задач к другим классам сложности. Поэтому в данном разделе мы упомянем некоторые основные результаты по NP-полноте некоторых задач на клеточных автоматах.

В работе [53] доказывается, что задача определения того, существует ли заполнение данного клеточного автомата, приводящее через *t* шагов к заполнению, содержащему данную подстроку длины *t*, является NP-полной. Там же доказывается, что задача о том, чтобы определить, существует ли для данного клеточного автомата заполнение, содержащее данную подстроку *s* длины *t*, переходящее за *t* шагов в заполнение, содержащее ту же подстроку, также является NP-полной.

В работе [54] исследовались сложность некоторых задач на так называемых аддитивных автоматах на графах, представляющих собой, по существу, обобщенные клеточные автоматы, ячейки которых являются элементами некоторого конечного аддитивного моноида, а локальная функция связи представляет собой сумму своих аргументов. Доказано, что для таких автоматов задача о существовании предыдущего состояния является NP-полной, если мощность этого моноида равна трем.

В работе [55] рассматривается задача определения по данному клеточному автомату и данной паре заполнений (X,Y), существует ли такое натуральное число t, что автомат перейдет из заполнения X в заполнение Y за t шагов. Причем рассматривается она для класса предсказуемых в слабом смысле (weakly-predictible) клеточных автоматов, т.е. таких, что состояние клеточного автомата через t шагов вычисляется за время $O((\log t)N^k)$, где N – число ячеек, а k – некоторая константа. Оказалось, что эта задача принадлежит классу coAM для двух подклассов предсказуемых в слабом смысле клеточных автоматов: являющихся инвертируемыми и являющихся аддитивными. Напомним здесь, что класс AM – это класс задач распознавания, которые могут быть решены за полиномиальное время с помощью протокола Артур–Мерлин с двумя сообщениями. Класс coAM – это дополнение к классу AM.

Перейдем теперь к результату [56], интересному в контексте обоснования стойкости криптоалгоритмов, основанных на обобщенных клеточных автоматах, связанному с исследованием вычислительной сложности задачи о восстановлении предыдущего состояния такого автомата. Пусть дан обобщенный клеточный автомат и его заполнение после первого шага $M(1)$. Назовем задачей о восстановлении предыдущего состояния обобщенного клеточного автомата задачу нахождения такого его начального заполнения $M(0)$, которое после первого шага перейдет в заполнение $M(1)$. Сформулируем теперь эту задачу в форме распознавания. Назовем задачей о существовании предыдущего состояния обобщенного клеточного автомата следующую задачу. Дан обобщенный клеточный автомат и его заполнение после первого шага $M(1)$. Распознать, существует ли его начальное заполнение $M(0)$, которое после первого шага перейдет в заполнение $M(1)$.

В работе [56] доказана теорема о том, что задача о существовании предыдущего состояния однородного обобщенного клеточного автомата является NP-полной. Соответственно, задача восстановления этого состояния является NP-трудной. При этом, NP-трудность этой задачи сохраняется, если рассматривать все обобщенные клеточные автоматы, отличные от классических. Этот результат достаточно важен для задачи обоснования стойкости криптографических алгоритмов, основанных на обобщенных клеточных автоматах.

4. Заключение

Итак, использование клеточных автоматов в качестве основы для криптографических алгоритмов выглядит весьма перспективным. Хотя одномерные клеточные автоматы, по-видимому, не позволяют обе-

DOI:10.21681/2311-3456-2022-1-37-48

спечить достаточную стойкость основанных на них симметричных криптографических алгоритмов, уже двухмерные автоматы выглядят в этом смысле гораздо лучше, а обобщенные клеточные автоматы позволяют построить симметричные криптографические алгоритмы, которые не только обеспечивают высокую криптостойкость, но и позволяют достичь очень высокой производительности при аппаратной реализации, а также низких требований к аппаратным ресурсам. Дальнейшие исследования как методов построения таких криптоалгоритмов, так и методов их анализа, представляются весьма перспективными.

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

Литература

1. Kauffman S. A. Metabolic stability and epigenesis in randomly constructed genetic nets // Journal of theoretical biology. – 1969. – Vol. 22, No. 3. – P. 437–467.
2. Aldana M., Coppersmith S., Kadanoff L. P. Boolean dynamics with random couplings // Perspectives and Problems in Nolinear Science. – Springer, 2003. – P. 23–89.
3. Gershenson C. Introduction to random boolean networks // arXiv preprint nlin/0408006. – 2004.
4. Bilke S., Sjunnesson F. Stability of the Kauffman model // Physical Review E. – 2001. – Vol. 65, No. 1. – P. 016129.
5. Socolar J. E., Kauffman S. A. Scaling in ordered and critical random boolean networks // Physical review letters. – 2003. – Vol. 90, No. 6. – P. 068702–1–068702–4.
6. Samuelsson B., Troein C. Superpolynomial growth in the number of attractors in Kauffman networks // Physical Review Letters. – 2003. – Vol. 90, No. 9. – P. 098701.
7. Mihaljev T., Drossel B. Scaling in a general class of critical random boolean networks // Physical Review E. – 2006. – Vol. 74, No. 4. – P. 046101.
8. Ключарёв П. Г. Обеспечение криптографических свойств обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2012. – № 3. – Режим доступа: http://technomag.edu.ru/doc/358973.html.
9. 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.
10. 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.
11. Ключарёв П. Г. О периоде обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2012. – № 2. – Режим доступа: http://technomag.edu.ru/doc/340943.html.
12. Ключарёв П. Г. Об устойчивости обобщенных клеточных автоматов к некоторым типам коллизий // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2014. – № 9. – С. 194–202. – Режим доступа: http://technomag.edu.ru/doc/727086.html.
13. Ключарёв П. Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2011. – № 10. – Режим доступа: http://www.technomag.edu.ru/doc/241308.html.
14. Ключарёв П. Г. Построение псевдослучайных функций на основе обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2012. – № 10. – С. 263–274.
15. Ключарёв П. Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2012. – № 12. – С. 361–374. – Режим доступа: http://engineering-science.ru/doc/517543.html.
16. Жуков А. Е. Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности. – 2017. – № 4(22). – С. 47–66. DOI:10.21681/2311-3456-2017-4-47-66
17. Ключарёв П. Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2013. – № 1. – С. 161–172.
18. Ключарёв П. Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. – 2017. – № 1(19). – С. 45–50. DOI: 10.21681/2311-3456-2017-1-45-50
19. Ключарёв П. Г. Построение алгоритмов выработки имитовставок на основе обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2016. – № 11. – С. 142–152. – Режим доступа: http://engineering-science.ru/doc/849590.html.
20. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // Bulletin of the American Mathematical Society. – 2006. – Vol. 43, No. 4. – P. 439–562.
21. 21. Ключарёв П. Г. Детерминированные методы построения графов Рамануджана, предназначенных для применения в криптографических алгоритмах, основанных на обобщённых клеточных автоматах // Прикладная дискретная математика. – 2018. – № 42. – С. 76–93.
22. Ключарёв П. Г. Построение случайных графов, предназначенных для применения в криптографических алгоритмах, основанных на обобщенных клеточных автоматах // Математика и математическое моделирование. – 2017. – № 3. – С. 77–90. – Режим доступа: https://www.mathmelpub.ru/jour/article/view/76.
23. Pizer A. K. Ramanujan graphs and Hecke operators // Bulletin of the American Mathematical Society. – 1990. – Vol. 23, No. 1. – P. 127–137.
24. Charles D., Lauter K., Goren E. Cryptographic hash functions from expander graphs // J. Cryptology. – 2009. – Vol. 22, No. 1. – P. 93–113.
25. Petit C. On Graph-Based Cryptographic Hash Functions: Ph. D. thesis / C. Petit ; Catholic University of Louvain. – 2009. – 286 p.
26. Ramanujan graphs in cryptography / Anamaria Costache, Brooke Feigon, Kristin Lauter et al. // Research Directions in Number Theory. – Springer, 2019. – P. 1–40.

27. Adj G., Ahmadi O., Menezes A. On isogeny graphs of supersingular elliptic curves over finite fields // Finite Fields and Their Applications. – 2019. – Vol. 55. – P. 268–283.
28. Sarnak P. Some applications of modular forms. – Cambridge University Press, 1990. – Vol. 99. – 111 p.
29. De Feo L., Jao D., Plut J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Journal of Mathematical Cryptology. – 2014. – Vol. 8, No. 3. – P. 209–247.
30. Постквантовый криптографический протокол выработки общего ключа, основанный на изогениях суперсингулярных эллиптических кривых / С. В. Гребнев, П. Г. Ключарёв, А. М. Коренева и др. // Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2021. – С. 99–103.
31. Ключарёв П. Г. Исследование стойкости блочных шифров, основанных на обобщенных клеточных автоматах, к линейному криптоанализу // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2013. – № 5. – С. 235–246. – Режим доступа: http://engineering-science.ru/doc/574231.html.
32. Ключарёв П. Г. Квантовые вычисления и атаки на криптоалгоритмы, основанные на обобщенных клеточных автоматах // Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2017. – С. 234–236.
33. Ключарёв П. Г. Исследование практической возможности решения связанных с криптоанализом задач на обобщенных клеточных автоматах алгебраическими методами // Математика и математическое моделирование. – 2017. – № 5. – С. 29–44.
34. Ключарёв П. Г. Исследование практической возможности решения одной задачи на обобщенных клеточных автоматах с использованием SAT-решателей // Машиностроение и компьютерные технологии. – 2018. – № 11. – С. 11–22. – Режим доступа: https://www.elibrary.ru/item.asp?id=37315433.
35. Ключарёв П. Г. Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2013. – № 10. – С. 299–314. – Режим доступа: http://engineering-science.ru/doc/624722.html.
36. Ключарёв П. Г. Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2014. – № 1. – С. 214–223. – Режим доступа: http://engineering-science.ru/doc/675812.html.
37. De Canniere C. Trivium: A stream cipher construction inspired by block cipher design principles // Information Security. – Springer, 2006. – P. 171–186.
38. Ключарёв П. Г. Производительность поточных шифров, основанных на клеточных автоматах, при реализации на графических процессорах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2016. – № 6. – С. 200–213. – Режим доступа: http://engineering-science.ru/doc/842091.html.
39. Ключарёв П. Г. Производительность древовидных криптографических хэш-функций, основанных на клеточных автоматах, при их реализации на графических процессорах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2016. – № 10. – С. 132–142. – Режим доступа: http://engineering-science.ru/doc/847891.html.
40. Ключарёв П. Г. О производительности блочных шифров, основанных на клеточных автоматах, при их реализации на графических процессорах // Радиооптика. – 2016. – № 6. – С. 24–34.
41. Shihua T. R. C. A finite automaton public key cryptosystem and digital signatures [j] // Chinese Journal of Computers. – 1985. – Vol. 6.
42. Агибалов Г. Конечные автоматы в криптографии // Прикладная дискретная математика. – 2009. – № Приложение к №2. – С. 43–73.
43. Bao F., Igarashi Y. Break finite automata public key cryptosystem // International Colloquium on Automata, Languages, and Programming / Springer. – 1995. – P. 147–158.
44. Dai Z. D., Ye D. F., Lam K. Y. Weak invertibility of finite automata and cryptanalysis on FAPKC // International Conference on the Theory and Application of Cryptology and Information Security / Springer. – 1998. – P. 227–241.
45. Kari J. Cryptosystems based on reversible cellular automata // Manuscript, August. – 1992.
46. Clarridge A., Salomaa K. A cryptosystem based on the composition of reversible cellular automata // International Conference on Language and Automata Theory and Applications / Springer. – 2009. – P. 314–325.
47. Santos T. Cellular automata and cryptography // Dissertao de Mestrado apresentada Faculdade de Cincias da Universidade do Porto em Cincia de Computadores. – 2014.
48. Guan P. Cellular automaton public-key cryptosystem // Complex Systems. – 1987. – Vol. 1. – P. 51–57.
49. A new public key encryption scheme based on layered cellular automata / Xing Zhang, Rongxing Lu, Hong Zhang, Chungen Xu // KSII Transactions on Internet and Information Systems (TIIS). – 2014. – Vol. 8, No. 10. – P. 3572–3590.
50. Чиликов А. А., Жуков А. Е., Верховский А. И. Исследование обратимых клеточных автоматов с конечной решеткой // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2019. – С. 354–360.
51. Жуков А. Е. Клеточные автоматы и запреты булевых функций // Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2021. – С. 108–119.
52. Arora S., Barak B. Computational Complexity: A Modern Approach. – Cambridge University Press, 2009. – 594 p.
53. Green F. NP-complete problems in cellular automata // Complex Systems. – 1987. – Vol. 1, No. 3. – P. 453–474.
54. Sutner K. Additive automata on graphs // Complex Systems. – 1988. – Vol. 2, No. 6. – P. 649–661.
55. Clementi A., Impagliazzo R. The reachability problem for finite cellular automata // Information processing letters. – 1995. – Vol. 53, No. 1. – P. 27–31.
56. Ключарёв П. Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. – 2012. – № 1. – Режим доступа: http://technomag.edu.ru/doc/312834.html.
57. Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 1. // Вопросы кибербезопасности. 2021. № 6 (46). С. 90-101. DOI: 10.21681/2311-3456-2021-6-90-101

CELLULAR AUTOMATA AND THEIR GENERALIZATIONS IN CRYPTOGRAPHY. PART 2.

Klyucharev P.G.[2]

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 cellular automata and their generalizations for the construction of cryptographic algorithms. The article consists of two parts.*

The first part was devoted to classical cellular automata and symmetric cryptographic algorithms based on them. It briefly discussed the history of the theory of cellular automata and its application in various scientific fields. A review of the works of a number of authors who proposed symmetric cryptographic algorithms and pseudorandom sequence generators based on one-dimensional cellular automata was presented. The security of such cryptographic algorithms turned out to be insufficient. The following was 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 were also mentioned.

This second part of the article is 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 is paid to interesting connections of generalized cellular automata, in the context of their use in cryptography, with the theory of expander graphs. Attention is also 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 are mentioned. In addition, an overview of asymmetric cryptoalgorithms based on cellular automata is 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, are also considered.

Keywords: *cellular automation, generalized cellular automation, stream cipher, block cipher, hash function, Ramanujan graph, public-key cryptography*

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

References

1. Kauffman S. A. Metabolic stability and epigenesis in randomly constructed genetic nets // Journal of theoretical biology. – 1969. – Vol. 22, No. 3. – P. 437–467.
2. Aldana M., Coppersmith S., Kadanoff L. P. Boolean dynamics with random couplings // Perspectives and Problems in Nolinear Science. – Springer, 2003. – P. 23–89.
3. Gershenson C. Introduction to random boolean networks // arXiv preprint nlin/0408006. – 2004.
4. Bilke S., Sjunnesson F. Stability of the Kauffman model // Physical Review E. – 2001. – Vol. 65, No. 1. – P. 016129.
5. Socolar J. E., Kauffman S. A. Scaling in ordered and critical random boolean networks // Physical review letters. – 2003. – Vol. 90, No. 6. – P. 068702–1–068702–4.
6. Samuelsson B., Troein C. Superpolynomial growth in the number of attractors in Kauffman networks // Physical Review Letters. – 2003. – Vol. 90, No. 9. – P. 098701.
7. Mihaljev T., Drossel B. Scaling in a general class of critical random boolean networks // Physical Review E. – 2006. – Vol. 74, No. 4. – P. 046101.
8. Klyucharev P. G. Obespechenie kriptograficheskix svojstv obobshhyonny'x kletochny'x avtomatov // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2012. – № 3. – Rezhim dostupa: http://technomag.edu.ru/doc/358973.html.
9. Suxinin B. M. Razrabotka i issledovanie vy'sokoskorostny'x generatorov psevdosluchajny'x ravnomerno raspredelenny'x dvoichny'x posledovatel'nostej na osnove kletochny'x avtomatov: Dis... kand. texn. nauk: 05.13.17 / Boris Mixajlovich Suxinin ; MGTU im. N.E'. Baumana. – M., 2011. – 224 s.
10. Suxinin B. M. Primenenie klassicheskix i neodnorodny'x kletochny'x avtomatov pri postroenii vy'sokoskorostny'x generatorov psevdosluchajny'x posledovatel'nostej // Proektirovanie i texnologiya e'lektronny'x sredstv. – 2009. – № 3. – S. 47–51.
11. Klyucharev P. G. O periode obobshhyonny'x kletochny'x avtomatov // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2012. – № 2. – Rezhim dostupa: http://technomag.edu.ru/doc/340943.html.
12. Klyucharev P. G. Ob ustojchivosti obobshhenny'x kletochny'x avtomatov k nekotory'm tipam kollizij // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2014. – № 9. – S. 194–202. – Rezhim dostupa: http://technomag.edu.ru/doc/727086.html.

2 Petr G. Klyucharev, Ph.D., associate professor of Information Security department, Bauman Moscow State Technical University, Moscow, Russia. E-mail: pk.iu8@yandex.ru

13. Klyucharev P. G. Kletochny'e avtomaty', osnovanny'e na grafax Ramanudzhana, v zadachax generacii psevdosluchajny'x posledovatel'nostej // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2011. – № 10. – Rezhim dostupa: http://www.technomag.edu.ru/doc/241308.html.
14. Klyucharev P. G. Postroenie psevdosluchajny'x funkcij na osnove obobshhyonny'x kletochny'x avtomatov // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2012. – № 10. – S. 263–274.
15. Klyucharev P. G. Blochny'e shifry', osnovanny'e na obobshhyonny'x kletochny'x avtomatax // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2012. – № 12. – S. 361–374. – Rezhim dostupa: http://engineering-science.ru/doc/517543.html.
16. Zhukov A. E. Kletochny'e avtomaty' v kriptografii. chast' 2 // Voprosy' kiberbezopasnosti. – 2017. – № 4(22). – S. 47–66.
17. Klyucharev P. G. Kriptograficheskie xe'sh-funkcii, osnovanny'e na obobshhyonny'x kletochny'x avtomatax // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2013. – № 1. – S. 161–172.
18. Klyucharev P. G. Metod postroeniya kriptograficheskix xe'sh-funkcij na osnove iteracij obobshhennogo kletochnogo avtomata // Voprosy' kiberbezopasnosti. – 2017. – № 1(19). – S. 45–50.
19. Klyucharev P. G. Postroenie algoritmov vy'rabotki imitovstavok na osnove obobshhyonny'x kletochny'x avtomatov // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2016. – № 11. – S. 142–152. – Rezhim dostupa: http://engineering-science.ru/doc/849590.html.
20. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // Bulletin of the American Mathematical Society. – 2006. – Vol. 43, No. 4. – P. 439–562.
21. Klyucharev P. G. Determinirovanny'e metody' postroeniya grafov Ramanudzhana, prednaznachenny'x dlya primeneniya v kriptograficheskix algoritmax, osnovanny'x na obobshhyonny'x kletochny'x avtomatax // Prikladnaya diskretnaya matematika. – 2018. – № 42. – S. 76–93.
22. Klyucharev P. G. Postroenie sluchajny'x grafov, prednaznachenny'x dlya primeneniya v kriptograficheskix algoritmax, osnovanny'x na obobshhenny'x kletochny'x avtomatax // Matematika i matematicheskoe modelirovanie. – 2017. – No 3. – S. 77–90. – Rezhim dostupa: https://www.mathmelpub.ru/jour/article/view/76.
23. Pizer A. K. Ramanujan graphs and Hecke operators // Bulletin of the American Mathematical Society. – 1990. – Vol. 23, No. 1. – P. 127–137.
24. Charles D., Lauter K., Goren E. Cryptographic hash functions from expander graphs // J. Cryptology. – 2009. – Vol. 22, No. 1. – P. 93–113.
25. Petit C. On Graph-Based Cryptographic Hash Functions: Ph. D. thesis / C. Petit ; Catholic University of Louvain. – 2009. – 286 p.
26. Ramanujan graphs in cryptography / Anamaria Costache, Brooke Feigon, Kristin Lauter et al. // Research Directions in Number Theory. – Springer, 2019. – P. 1–40.
27. Adj G., Ahmadi O., Menezes A. On isogeny graphs of supersingular elliptic curves over finite fields // Finite Fields and Their Applications. – 2019. – Vol. 55. – P. 268–283.
28. Sarnak P. Some applications of modular forms. – Cambridge University Press, 1990. – Vol. 99. – 111 p.
29. De Feo L., Jao D., Plut J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Journal of Mathematical Cryptology. – 2014. – Vol. 8, No. 3. – P. 209–247.
30. Postkvantovy'j kriptograficheskij protokol vy'rabotki obshhego klyucha, osnovanny'j na izogeniyax supersingulyarny'x e'llipticheskix krivy'x / S. V. Grebnev, P. G. Klyucharev, A. M. Koreneva i dr. // Bezopasny'e informacionny'e texnologii. Sbornik trudov XI mezhdunarodnoj nauchno-texnicheskoj konferencii. – M.: MGTU im. N.E'. Baumana, 2021. – S. 99–103.
31. Klyucharev P. G. Issledovanie stojkosti blochny'x shifrov, osnovanny'x na obobshhenny'x kletochny'x avtomatax, k linejnomu kriptoanalizu // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2013. – No 5. – S. 235–246. – Rezhim dostupa: http://engineering-science.ru/doc/574231.html.
32. Klyucharev P. G. Kvantovy'e vy'chisleniya i ataki na kriptoalgoritmy', osnovanny'e na obobshhenny'x kletochny'x avtomatax // Bezopasny'e informacionny'e texnologii. Sbornik trudov Vos'moj vserossijskoj nauchno-texnicheskoj konferencii. – M.: MGTU im. N.E'. Baumana, 2017. – S. 234–236.
33. Klyucharev P. G. Issledovanie prakticheskoj vozmozhnosti resheniya svyazanny'x s kriptoanalizom zadach na obobshhenny'x kletochny'x avtomatax algebraicheskimi metodami // Matematika i matematicheskoe modelirovanie. – 2017. – No 5. – S. 29–44.
34. Klyucharev P. G. Issledovanie prakticheskoj vozmozhnosti resheniya odnoj zadachi na obobshhenny'x kletochny'x avtomatax s ispol'zovaniem SAT-reshatelej // Mashinostroenie i komp'yuterny'e texnologii. – 2018. – № 11. – S. 11–22. – Rezhim dostupa: https://www.elibrary.ru/item.asp?id=37315433.
35. Klyucharev P. G. Proizvoditel'nost' i e'ffektivnost' apparatnoj realizacii potochny'x shifrov, osnovanny'x na obobshhenny'x kletochny'x avtomatax // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2013. – No 10. – S. 299–314. – Rezhim dostupa: http://engineering-science.ru/doc/624722.html.
36. Klyucharev P. G. Realizaciya kriptograficheskix xe'sh-funkcij, osnovanny'x na obobshhenny'x kletochny'x avtomatax, na baze PLIS: proizvoditel'nost' i e'ffektivnost' // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2014. – No 1. – S. 214–223. – Rezhim dostupa: http://engineering-science.ru/doc/675812.html.
37. De Canniere C. Trivium: A stream cipher construction inspired by block cipher design principles // Information Security. – Springer, 2006. – P. 171–186.
38. Klyucharev P. G. Proizvoditel'nost' potochny'x shifrov, osnovanny'x na kletochny'x avtomatax, pri realizacii na graficheskix processorax // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2016. – No 6. – S. 200–213. – Rezhim dostupa: http://engineering-science.ru/doc/842091.html.
39. Klyucharev P. G. Proizvoditel'nost' drevovidny'x kriptograficheskix xe'sh-funkcij, osnovanny'x na kletochny'x avtomatax, pri ix realizacii na graficheskix processorax // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2016. – No 10. – S. 132–142. – Rezhim dostupa: http://engineering-science.ru/doc/847891.html.
40. Klyucharev P. G. O proizvoditel'nosti blochny'x shifrov, osnovanny'x na kletochny'x avtomatax, pri ix realizacii na graficheskix processorax // Radiooptika. – 2016. – No 6. – S. 24–34.
41. Shihua T. R. C. A finite automaton public key cryptosystem and digital signatures [j] // Chinese Journal of Computers. – 1985. – Vol. 6.
42. Agibalov G. Konechny'e avtomaty' v kriptografii // Prikladnaya diskretnaya matematika. – 2009. – № Prilozhenie k No 2. – S. 43–73.
43. Bao F., Igarashi Y. Break finite automata public key cryptosystem // International Colloquium on Automata, Languages, and Programming / Springer. – 1995. – P. 147–158.

44. Dai Z. D., Ye D. F., Lam K. Y. Weak invertibility of finite automata and cryptanalysis on FAPKC // International Conference on the Theory and Application of Cryptology and Information Security / Springer. – 1998. – P. 227–241.
45. Kari J. Cryptosystems based on reversible cellular automata // Manuscript, August. – 1992.
46. Clarridge A., Salomaa K. A cryptosystem based on the composition of reversible cellular automata // International Conference on Language and Automata Theory and Applications / Springer. – 2009. – P. 314–325.
47. Santos T. Cellular automata and cryptography // Dissertao de Mestrado apresentada Faculdade de Cincias da Universidade do Porto em Cincia de Computadores. – 2014.
48. Guan P. Cellular automaton public-key cryptosystem // Complex Systems. – 1987. – Vol. 1. – P. 51–57.
49. A new public key encryption scheme based on layered cellular automata / Xing Zhang, Rongxing Lu, Hong Zhang, Chungen Xu // KSII Transactions on Internet and Information Systems (TIIS). – 2014. – Vol. 8, No. 10. – P. 3572–3590.
50. Chilikov A. A., Zhukov A. E., Verxovskij A. I. Issledovanie obratimy'x kletochny'x avtomatov s konechnoj reshetkoj // Bezopasny'e informacionny'e texnologii. Sbornik trudov Desyatoj mezhdunarodnoj nauchno-texnicheskoj konferencii. – M.: MGTU im. N.E'. Baumana, 2019. – S. 354–360.
51. Zhukov A. E. Kletochny'e avtomaty' i zaprety' bulevy'x funkcij // Bezopasny'e informacionny'e texnologii. Sbornik trudov XI mezhdunarodnoj nauchno-texnicheskoj konferencii. – M.: MGTU im. N.E'. Baumana, 2021. – S. 108–119.
52. Arora S., Barak B. Computational Complexity: A Modern Approach. – Cambridge University Press, 2009. – 594 p.
53. Green F. NP-complete problems in cellular automata // Complex Systems. – 1987. – Vol. 1, No. 3. – P. 453–474.
54. Sutner K. Additive automata on graphs // Complex Systems. – 1988. – Vol. 2, No. 6. – P. 649–661.
55. Clementi A., Impagliazzo R. The reachability problem for finite cellular automata // Information processing letters. – 1995. – Vol. 53, No. 1. – P. 27–31.
56. Klyucharev P. G. NP-trudnost' zadachi o vosstanovlenii predy'dushhego sostoyaniya obobshhennogo kletochnogo avtomata // Nauka i obrazovanie. MGTU im. N.E'. Baumana. E'lektron. zhurn. – 2012. – No 1. – Rezhim dostupa: http://technomag.edu.ru/doc/312834.html.
57. Klyucharev P.G. Kletochnye avtomaty i ih obobshcheniya v zadachah kriptografii. CHast 1. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021. No 6 (46), pp. 90-101. DOI: 10.21681/2311-3456-2021-6-90-101.

Примечание редакции

По оценкам слепого рецензирования данной статьи (часть 1 - №6-2021 и часть 2 - №1-2022) рецензентом были отмечены следующие рекомендации:

1. В работе, на наш взгляд, несколько тенденциозно представлены работы зарубежных научных школ, в ущерб отечественным научным школам, в том числе родоначальникам русскоязычной терминологии КА (однородных структур в русскоязычной терминологии), и особенно весьма лаконично упомянуты ученые, находящиеся у истоков становления теории КА в СССР.

Указанное свидетельствует о некоторой неполноте опубликованного обзора в исторической ретроспективе.

Из относительно недавних публикаций можно было рекомендовать, например, две публикации:

- *Аладьев В.З. Классические однородные структуры. Клеточные автоматы.- CA: Palo Alto, Fultus Corporation, 2009, 536 с. (на русском языке).*
- *Матюшкин И. В., Заплетина М. А. Обзор по тематике клеточных автоматов на базе современных отечественных публикаций. // Компьютерные исследования и моделирование. 2019. Т. 11, No 1. С. 9–57 DOI: 10.20537/2076-7633-2019-11-1-9-57.*

2. Полагаю, что публикация бы выиграла, если автор более полно учел и материалы индийского математика Palash Sarkar:

- *Sarkar P. A Brief History of Cellular Automata. ACM Computing Surveys, Vol. 32, No. 1, March 2000. URL: https://www.cs.ucf.edu/~dcm/Teaching/COT4810-Spring2011/Literature/CellularAutomata.pdf)*