КЛЕТОЧНЫЕ АВТОМАТЫ В КРИПТОГРАФИИ Часть 2.

Жуков А.Е.[1]

Статья является продолжением публикации обзора применения клеточных автоматов в различных научно–технических областях, в первую очередь в области криптографии [1]. Отмечается, что клеточные автоматы выступают как самостоятельные объекты теоретического изучения, так и в качестве инструмента для моделирования в науке и технике. В основе популярности клеточных автоматов лежит их сравнительная простота в сочетании с большими возможностями для моделирования совокупности взаимосвязанных однородных объектов. Кроме того, клеточные автоматы, являясь параллельными структурами, прекрасно подходят для моделирования дискретных параллельных процессов, для создания параллельных алгоритмов обработки информации и представляют интерес в качестве основы вычислительной техники с высокопараллельной архитектурой.

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

DOI: 10.21581/2311-3456-2017-4-47-66

Клеточные автоматы и криптография

Пожалуй, нет такого раздела математики, который не применяли или хотя бы не пытались применить в криптографических исследованиях. Как отмечалось в первой части исследования, не осталась в стороне и теория клеточных автоматов (КлА) [1]. После первого приложения теории КлА к криптографии [2] и последовавшей в период середины 80-х – начала 90-х годов волны публикаций в этом направлении, наступило некоторое охлаждение интереса к этой тематике и, как следствие, относительный спад в числе публикаций. Объясняется это тем, что в первых криптографических алгоритмах, использовавших модель КлА, были обнаружены слабости. Часть работ, как это порой бывает с направлениями, ставшими вдруг «модными», оказалась просто элементарно безграмотной и содержала грубейшие ошибки, поскольку работы зачастую писались не профессиональными криптографами, а людьми, имевшими о криптографии самое поверхностное представление. Все это не могло не сказаться на «авторитете» этой тематики.

Однако в последнее время вновь наблюдается рост интереса криптографического сообщества к использованию в криптографии клеточно-автоматных моделей. Количество работ, посвященных приложению КлА к криптографии, за последние годы вновь резко выросло. Все это объясняется само́й природой КлА и, прежде всего, свойствами параллельности и локальности. Они позволяют организовать параллельную обработку существенных порций информации с помощью достаточно скромных вычислительных ресурсов. Это соответствует современной тенденции в развитии информационных технологий, когда мы имеем дело с огромным потоком са́мой разнообразной информации из самых разных источников. Эта информация порой требует обработки в условиях весьма ограниченных вычислительных ресурсов (как то, например, смарт-карты или радиочастотные метки, имеющие выход в Интернет), что образует сферу так называемого Интернета Вещей. И здесь клеточные автоматы могут найти самое широкое применение в качестве высокоскоростных и не требовательных к ресурсам шифровальных средств, если удастся в полной мере реализовать их возможности, связанные с присущим им «природным» параллелизмом вычислений.

ГПСП на основе классических клеточных автоматов

Первые исследования в области клеточных автоматов, их свойств и возможностей их применения как генераторов псевдослучайных последовательностей (ГПСП) принадлежат С. Вольфраму и относятся к одномерным клеточным автоматам [3]. Вольфрамом и рядом других авторов была рассмотрена возможность применения подобных одномерных КлА в качестве генераторов гаммы поточного шифрования.

ГПСП на основе одномерных клеточных автоматов

Рассмотрим предложенный Вольфрамом ГПСП подробнее. Одномерный клеточный автомат

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

представляет собой массив из N циклически соединенных ячеек памяти $s = [m_0, m_1, \dots, m_{N-1}]$, каждая из которых может принимать значения из множества $\Omega = \{0,1\}$. В процессе функционирования КлА все ячейки меняют свои значение синхронно и одновременно. Значение i-й ячейки на t-м такте работы будем обозначать $m_i(t)$. Тогда значение i-й ячейки на (t+1)-ом такте работы определяется локальной функцией связи

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

$$\oplus\, m_i(t) \cdot m_{i+1}(t),\ 0 \le i < N,\ t = 0,1,\dots,$$

где вычисление индексов осуществляются по модулю N (т.к. массив ячеек памяти «закольцован»). Вектором инициализации генератора является набор $s(0) = [m_0(0), m_1(0), \dots, m_{N-1}(0)]$, образованный начальным заполнением ячеек памяти.

Для формирования выходной последовательности $\{\gamma(t)\}$ генератора используется съем с одной зафиксированной ячейки:

$$\gamma(t) = m_k(t), t = 1,2,\dots.$$

Таким образом, генератор вырабатывает выходную последовательность со скоростью 1 бит за 1 такт работы.

Вольфрам рассматривал клеточные автоматы с различным числом ячеек памяти и, основываясь на эмпирических данных, пришел к выводу, что при больших значениях N большинство состояний такого автомата лежит на одном цикле длины $\sim 2^N$.

Через некоторое время Мейер (Meier W.) и Стаффельбах (Staffelbach O.) представили атаку на этот шифр [4]. Для значений $N \le 500$ эта атака может быть реализована на обычном ПК в реальное время. Кроме того, Бардел (Bardell P.H.) [5] доказал, что линейная сложность выходной последовательности такого генератора совпадает с числом его ячеек памяти, что также не позволяет считать данный генератор криптографически безопасным.

В последующем различными авторами было предложено много схем поточного шифрования с генератором ключевого потока на базе классического одномерного клеточного автомата. Как правило, такие генераторы демонстрируют достаточно хорошие статистические свойства и эффективную аппаратную реализацию. Тем не менее, они обладают и рядом существенных недостатков, таких как:

- недостаточная изученность свойств КлА, обеспечивающих криптографическую стойкость соответствующего алгоритма;
- неэффективная программная реализация на последовательных вычислительных устройствах[2)].

Отметим, что практически все генераторы на базе одномерного клеточного автомата, привлекшие внимание криптоаналитиков, через некоторое время оказались взломанными (например, [6-8]). Невзломанными, по всей видимости, остались лишь схемы, анализом которых никто, кроме самих авторов, не занимался.

В настоящее время одномерные клеточные автоматы используются в составе генератора псевдослучайных последовательностей в математическом пакете Wolfram Mathematica, разработанном компанией Wolfram Research[3], однако в остальном они не получили широкого распространения.

ГПСП на основе двумерных клеточных автоматов

Возможность применения двумерных клеточных автоматов в качестве генераторов гаммы поточного шифрования рассматривалась в зарубежной литературе достаточно редко, в качестве примера можно привести лишь работы [9, 10]. Наиболее существенный вклад в развитие этого направления содержится в работах [11-15]. Так, для характеристики криптографических свойств двумерных клеточного автомата было применено понятие лавинного эффекта, введенное в 1973 году Х. Фейстелем (Feistel H.) [16] для блочных шифров. С неформальной точки зрения – это свойство преобразований, при котором небольшие изменения входных данных влекут за собой значительные изменения выходных данных. Оно играет важнейшую роль в криптографии при изучении свойств блочных шифров и хэш-функций.

В нашем случае для измерения лавинного эффекта рассматриваются два тождественных клеточных автомата $\boldsymbol{A}$ и $\widehat{\boldsymbol{A}}$. Пусть $s(t) = (m_1(t), m_2(t), \dots, m_N(t))$ и $\hat{s}(t) = (\hat{m}_1(t), \hat{m}_2(t), \dots, \hat{m}_N(t))$ – внутренние состояния этих автоматов в момент времени t, где $m_i(t)$ и $\hat{m}_i(t)$ – соответствующие заполнения ячеек памяти в момент времени t, а N – число ячеек памяти в автоматах $\boldsymbol{A}$ и $\widehat{\boldsymbol{A}}$. Локальные функции связи, разумеется, также совпадают. Пусть начальные состояния $s(0)$ и $\hat{s}(0)$ различаются в заполнении только одной ячейки, т.е. удовлетворяют условию:

$$m_k(0) \ne \hat{m}_k(0) \text{ и } m_i(0) = \hat{m}_i(0)\ \ \forall i \ne k.$$

В работе [13] для количественного описания лавинного эффекта в классических КлА были вве-

2 Неэффективность связана с последовательным характером работы вычислителя.

3 http://reference.wolfram.com/

дены понятия *интегральной* и *пространственной* характеристик лавинного эффекта.

Интегральная характеристика лавинного эффекта $\eta(t)$ равна отношению числа различающихся в данный момент времени одноименных ячеек к общему числу ячеек клеточного автомата:

$$\eta(t) = \frac{1}{N}\sum_{i=1}^{N}(m_i(t) \oplus \hat{m}_i(t)),$$

где Σ – обычное арифметическое сложение, а $\oplus$ – сложение по модулю 2.

Интегральная характеристика лавинного эффекта ограничена сверху:

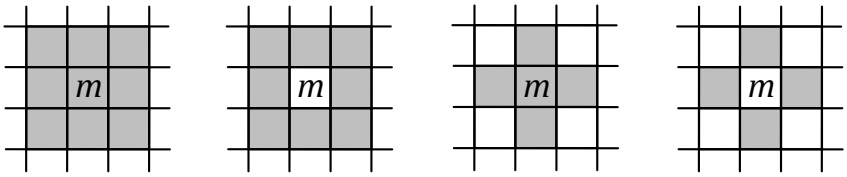
$$\eta(t) \le \begin{cases} \frac{1}{2N}\frac{|\psi|^{t+1}-1}{|\psi|-1}, & \frac{|\psi|^{t+1}-1}{|\psi|-1} \le N, \\ \frac{1}{2}, & \frac{|\psi|^{t+1}-1}{|\psi|-1} > N, \end{cases}$$

где $|\psi|$ – мощность окрестности каждой ячейки (для классических КлА данные мощности равны для любой из ячеек).

В свою очередь, *пространственная характеристика* $\mu(t)$ показывает скорость, с которой изменения распространяются по решетке клеточного автомата.

Там же было введено *понятие оптимального лавинного эффекта: оптимальным лавинным эффектом называется лавинный эффект при котором* изменения распространяются по решетке КлА равномерно во всех направлениях с максимально возможной скоростью, и при этом значение каждой ячейки изменяется с вероятностью 1/2.

Далее в указанных работах было произведено исследование характеристик лавинного эффекта для двумерных КлА в зависимости от размера и типа выбранной окрестности (рис. 3). Результаты этого исследования приведены на рис. 4 и 5.



(а) (б) (в) (г)

Рис. 3 *– Некоторые типы окрестности радиуса r = 1 для ячейки m двумерного КлА:*
а) полная окрестность (окрестность Мура)
б) квазиполная окрестность Мура
в) окрестность фон Неймана
г) неполная окрестность фон Неймана

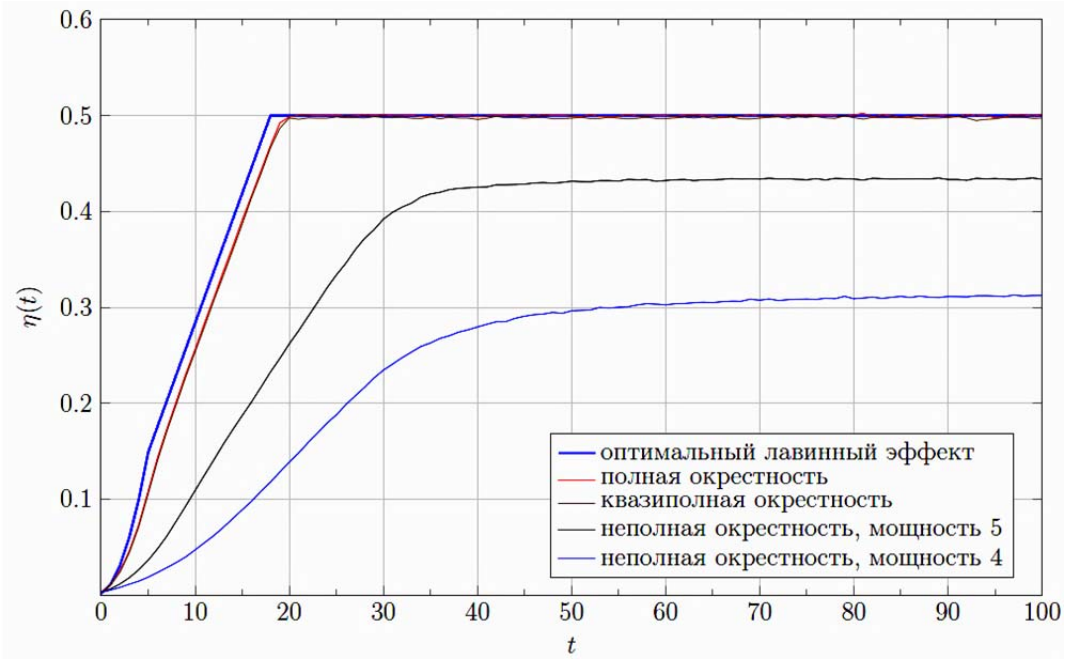


Рис. 4 *– Интегральные характеристики лавинного эффекта в классических двумерных КлА*

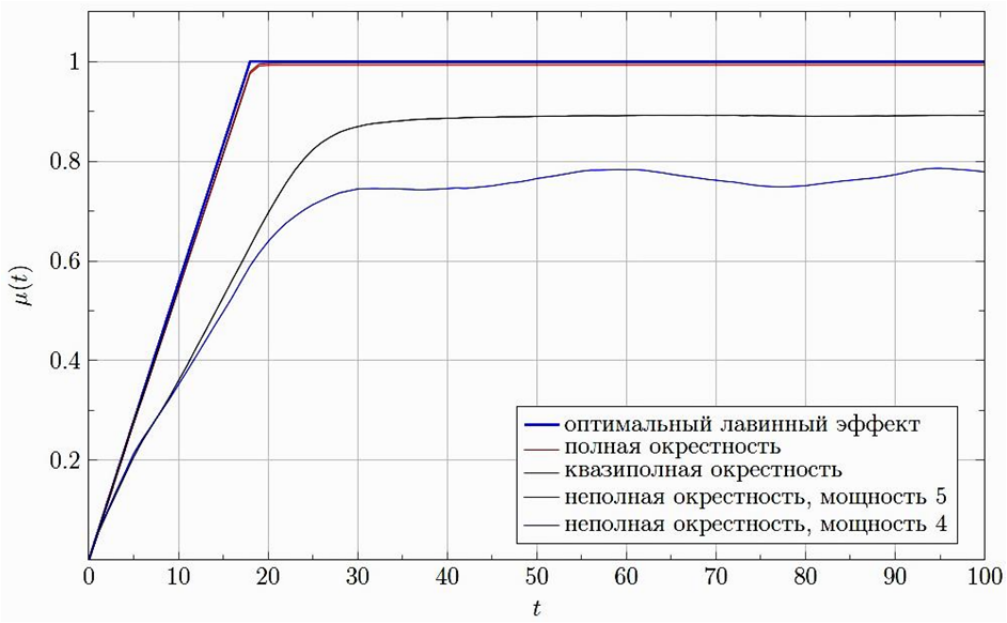


***Рис. 5** – Пространственные характеристики лавинного эффекта в классических двумерных КлА*

В итоге для 2-мерных клеточных автоматов в названных ранее работах [11-15] было:

- исследовано влияние веса локальной функции связи на распределение значений ячеек памяти КлА; сформулирован, доказан и подтвержден эмпирически критерий сохранения равномерности распределения;
- для количественного описания лавинного эффекта в классических КлА были введены понятия интегральной и пространственной характеристик лавинного эффекта, а также понятие оптимального лавинного эффекта;
- получено теоретическое описание характеристик оптимального лавинного эффекта и эмпирические зависимости характеристик лавинного эффекта от выбора окрестностей ячеек; показано, что клеточные автоматы обладают свойством размножения изменений;
- разработаны новые методы генерации псевдослучайных последовательностей; осуществлен синтез ГПСП и обоснован выбор его параметров; указан способ обеспечения заданного периода выходной последовательности;
- исследованы статистические свойства выходных последовательностей разработанных генераторов; определены конкретные локальные функции связи и окрестности ячеек КлА, обеспечивающие хорошие статистические свойства выходных последовательностей; подтверждено соответствие статистических свойств современным требованиям;
- разработана и изготовлена в виде устройства на ПЛИС высокоскоростная аппаратная реализация предложенных генераторов на базе 2-мерных клеточных автоматов, превосходящая аналоги по быстродействию (см. рис. 7 – график ККлА).

Обобщенные клеточные автоматы

Нами уже было отмечено, что клеточные автоматы имеют приложения во многих отраслях науки, таких как физика, химия, биология, информатика и т.д. В получаемых моделях удается достаточно точно воспроизводить многие природные явления, моделируя механизмы, лежащие в их основе. Однако если для большинства приложений важна регулярная структура решетки ячеек памяти, для криптографических приложений любая регулярность, как правило, ведет к снижению криптостойкости. По-видимому, это главная причина, по которой классические КлА, несмотря на многочисленные попытки, широкого применения в криптографии не нашли. Отказ от регулярной структуры для массива ячеек памяти лишает КлА некоторых преимуществ, но больше подходит для криптографических приложений, где регулярность оказывается вредной.

Как уже упоминалось выше, «клеточные автоматы изобретались много раз под разными названиями» [17]. Обобщенный клеточный автомат впервые появился в 1969 г. в работах Стюарта Кауффмана (Kauffman S.A.) под именем «булевой сети» (Boolean network) и предназначался для моделирования генетических процессов в биологии [18], а затем был описан в работе [11], где был на-

зван «неоднородным клеточным автоматом» (в данной работе термин «неоднородный клеточный автомат» будет использоваться в другом смысле).

Математически обобщенный КлА можно описать следующим образом.

Пусть задан ориентированный граф $G = (V, E)$, где $V = \{v_1, \dots v_N\}$ — множество вершин графа, E — множество дуг. Пусть δ_i – полустепень захода для вершины v_i, при этом входящие в вершину дуги пронумерованы числами 1,…, δ_i. Будем считать, что с каждой вершиной v_i связана ячейка памяти, содержащая булеву переменную m_i, и булева функция $f_i(x_1, \dots, x_{\delta_i})$ — локальная функция связи *i*-й вершины.

Обобщенный клеточный автомат – это автономный автомат, его внутренним состоянием в момент времени t называется заполнение массива ячеек $(m_1(t), m_2(t), \dots, m_N(t))$. Функция переходов является отображением множества состояний в себя и определяет следующее состояние автомата как функцию от текущего состояния. При этом заполнение ячеек памяти обобщенного КлА описывается уравнением:

$$m_i(t) = f_i\left(m_{n(i,1)}(t-1), m_{n(i,2)}(t-1), \dots, \dots, m_{n(i,\delta_i)}(t-1)\right),$$

где $m_i(t)$ — состояние *i*-й ячейки памяти в момент времени t, $n(i,j)$ — номер вершины, из которой исходит дуга, входящая в вершину *i* и имеющая номер *j*.[4])

Однородный обобщенный клеточный автомат – это обобщенный клеточный автомат, граф которого является регулярным по входу (т.е. число дуг, заходящих в вершину – одно и то же для всех вершин) и при этом локальная функция связи для всех ячеек одинакова. В противном случае обобщенный клеточный автомат будет называться *неоднородным*.

Выходом однородного обобщенного КлА на шаге с номером t будем считать значения r фиксированных ячеек памяти в этот момент времени: $\mathbf{y}(t) = (m_{i_1}(t), m_{i_2}(t), \dots, m_{i_r}(t))$. Последовательность: $\mathbf{y}(t_0)$, $\mathbf{y}(t_0+1)$, $\mathbf{y}(t_0+2)$ … образует выходную последовательностью клеточного автомата.

Переход к обобщенному клеточному автомату позволяет не только сохранить все преимущества классического КлА, но и улучшить многие его характеристики. Для обобщенного КлА выполняются следующие свойства:

- **Параллельность вычислений.** Это дискретная динамическая система с параллельными вычислениями значений ячеек памяти – свойство, совершенно аналогичное классическому случаю;
- **Свойство локальности.** В отличие от классического клеточного автомата, ячейки памяти обобщенного КлА могут быть соединены любым способом, подходящим для решения поставленной задачи, т.е. «окрестность» понимается не в геометрическом, а в теоретико-графовом смысле;
- **Свойство неоднородности.** В общем случае, функции изменения состояния ячеек могут быть различными для разных ячеек и обладать при этом любыми требуемыми свойствами. Однако локальные функции связи могут быть и одинаковыми, как в случае с классическими клеточными автоматами что, во-первых, удобно при практической реализации клеточного автомата, а во-вторых, упрощает анализ его поведения.

Свойства обобщенных клеточных автоматов

При моделировании с помощью КлА природных процессов (например, в биологии) наибольший интерес представляют аттракторы – устойчивые в том или ином смысле конфигурации заполнений ячеек памяти. Основные направления исследований в этом случае сводились к поиску условий, вызывающих их появление. Так было и при изучении булевых сетей (первоначальное название обобщенных клеточных автоматов) – [19-25]. В то же время для криптографии наличие аттракторов – ситуация катастрофическая. Криптографическим идеалом является случайное равновероятное заполнение всех ячеек памяти, и основные усилия исследователей направлены на поиск условий, обеспечивающих такое предельное распределение.

Важнейшим фактором, определяющим поведение однородного обобщенного клеточного автомата, является его структура, которая полностью определяется структурой соответствующего графа. Соответственно, и криптографические свойства обобщенного клеточного автомата как преобразования, реализующего некоторую однонаправленную функцию, и свойство быть «удобно и эффективно реализуемым» так же напрямую зависят от структуры графа и свойств локальной функции связи.

Так введенные в [13] для классических клеточ-

4 В работах [26-28] основу обобщенного КлА составлял неориентированный граф. В этом случае ячейки памяти, соединенные ребром, влияют друг на друга, что не противоречит приведенному выше определению обобщенного КлА но, в принципе, предоставляет дополнительные возможности для проведения криптоанализа.

ных автоматов, интегральная и пространственная характеристики лавинного эффекта были в [15, 26] перенесены на случай обобщенных клеточных автоматов. Как и в случае двумерного клеточного автомата, для определения интегральной и пространственной характеристик рассматриваются два идентичных клеточных автомата, работающие на паре начальных заполнений, различающихся в заполнении только одной ячейки. Пусть эта ячейка соответствует вершине v_1 графа G, задающего наш автомат.

Интегральной характеристикой называется зависящая от номера такта величина $\eta(t)$, равная отношению числа несовпадающих значений одноименных ячеек в этих двух автоматах к числу ячеек клеточного автомата.

Пространственной характеристикой лавинного эффекта для обобщенного клеточного автомата называется зависимость отношения расстояния от вершины v_1 до самой дальней вершины, для которой значения соответствующих ячеек в двух автоматах не совпадают, к эксцентриситету вершины v_1:

$$\mu(t) = \frac{1}{e(1)} \cdot \left(\max_j \left(m_j^{(1)}(t) \oplus m_j^{(2)}(t) \right) \cdot \Delta(1,j) \right),$$

где $\Delta(i,j)$ – длина минимального пути из вершины i в вершину j, а $e(i)$ – эксцентриситет вершины v_i.[5])

Для обеспечения должного уровня лавинного эффекта, а также для обеспечения хороших статистических характеристик выходной последовательности необходимо, чтобы с ростом t характеристики $\eta(t) \to 1/2$, а $\mu(t) \to 1$, причем желательно, чтобы приближение к указанным пределам происходило максимально быстро. Чтобы уменьшить время, необходимое для этого, следует использовать клеточный автомат, граф которого имеет как можно меньший диаметр (при заданных значениях N и δ).

ГПСП на основе обобщенных клеточных автоматов

В [13, 15], наряду с ГПСП на основе классических клеточных автоматов, были рассмотрены ГПСП на основе обобщенных однородных клеточных автоматов. Было продемонстрировано заметное преимущество ГПСП на основе обобщенных клеточных автоматов по сравнению с классическими в быстродействии и, особенно, в эффективности аппаратной реализации на ПЛИС (FPGA).

Предложенный ГПСЧ представляет собой два параллельно работающих обобщенных однородных клеточных автомата A_1 и A_2 дополненных регистром сдвига с линейной обратной связью. На каждом такте работы клеточные автоматы A_1 и A_2 вырабатывают по 256 бит двоичных последовательностей, которые складываются побитно, а результат сложения подается на выход генератора. Поскольку последовательности, вырабатываемые клеточными автоматами, могут рассматриваться как независимые, сложение позволяет улучшить статистические свойства выходной последовательности генератора.

Для исследования статистических свойств генераторов был использован набор специализированных тестов, разработанный Национальным институтом стандартов и технологий США[6]. Набор включает в себя 15 статистических тестов и предназначен для тестирования выходных последовательностей криптографических генераторов с предъявлением наиболее жестких требований. В результате указанных ранее исследований были определены конкретные графы и локальные функции связи, при которых разработанные генераторы успешно проходят весь набор статистических тестов.

Физические характеристики прототипов аппаратной реализации

В ходе работ [13, 15], были так же разработаны прототипы аппаратной реализации генератора псевдослучайных последовательностей на основе классических клеточных автоматов (в терминологии автора – ККлА) и генератора псевдослучайных последовательностей на основе обобщенных однородных клеточных автоматов (в терминологии автора – НКлА). Для практической реализации предложенных ГПСП была выбрана микросхема FPGA Cyclone II (EP2C35F672C6) корпорации Altera, относящаяся к семейству недорогих ПЛИС начального уровня. Основные характеристики микросхемы приведены в табл. 1.

В терминологии Altera[7] ячейки ПЛИС называются логическими элементами (logic elements, LE). Каждый логический элемент микросхемы Cyclone II включает следующие основные компоненты (см. рис. 6):

5 Эксцентриситетом $e(v)$ вершины v графа G называется наибольшее из расстояний от вершины v до других вершин графа. Тогда радиус графа $r(G)$ есть наименьший из эксцентриситетов вершин в графе G, а диаметр графа $d(G)$ – наибольший из эксцентриситетов.

6 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. – NIST SP 800-22, Rev.1a, 2010.

7 Cyclone II Device Handbook

Таблица 1.
Основные характеристики микросхемы EP2C35F672C6

Параметр	Значение
Количество ячеек	33 216
Количество блоков памяти M4K (4 Кб)	105
Число выводов микросхемы, доступных пользователю	475

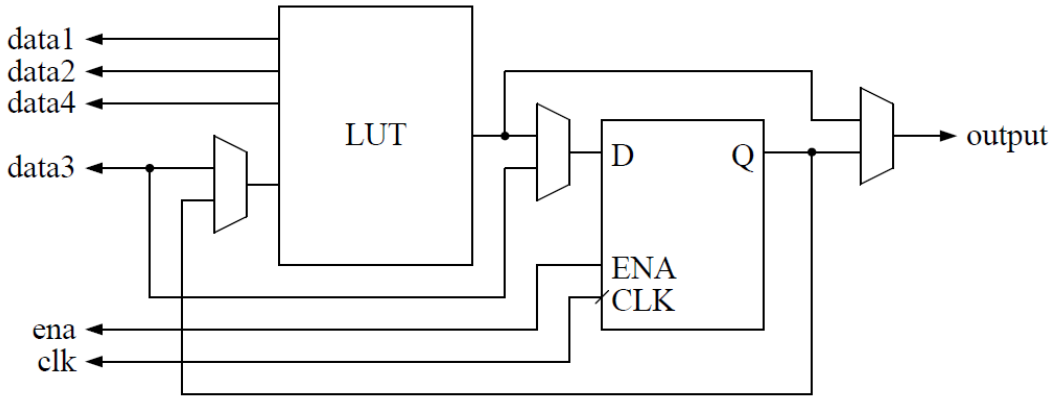


***Рис. 6** – Структура LE – логического элемента FPGA Altera Cyclone II*

- таблицу преобразования (look-up table, LUT) с 4 входами, позволяющую реализовать произвольную булеву функцию от четырех аргументов;
- программируемый триггер, способный функционировать в режиме D, T, JK или RS;
- программируемые внутренние связи.

Для генераторов ККлА и генераторов НКлА автором [13, 15] были построены прототипы аппаратной реализации на указанной микросхеме. Номинальное быстродействие прототипов составило 23,8 Гбит/с на тактовой частоте 100 МГц. При этом оно может быть увеличено до 33,4 Гбит/с для генераторов ККлА и до 35,5 Гбит/с для генераторов НКлА за счет увеличения тактовой частоты работы схемы без изменения самой реализации. Основные характеристики разработанных прототипов приведены в табл. 2.

Таблица 2.
Основные характеристики прототипа реализации генераторов псевдослучайных последовательностей на основе клеточных автоматов

Параметр	Генератор ККлА	Генератор НКлА
Характеристики быстродействия		
Номинальная тактовая частота	100 МГц	100 МГц
Номинальное быстродействие	23,8 Гбит/с	23,8 Гбит/с
Максимальная тактовая частота*)	140 МГц	149 МГц
Максимальное быстродействие	33,4 Гбит/с	35,5 Гбит/с
Использование ресурсов FPGA		
Количество задействованных логических элементов / Общее количество логических элементов микросхемы (в процентах)	22 004 / 33 126 (66%)	1 198 / 33 126 (4%)
Комбинационных без триггера	21 067	561
Триггеров без комбинационной части	0	0
Триггеров с комбинационной частью	937	637
Количество логических элементов в блоке generator/ Общее количество логических элементов микросхемы (в процентах)	21 892 / 33 126 (66%)	1 084 / 33 126 (3%)
*) По результатам статического анализа временных задержек в среде Altera Quartus II		

Сравнение с существующими аналогами

Было проведено сравнение полученных реализаций разработанных алгоритмов генерации псевдослучайных последовательностей (ККлА и НКлА) с аппаратными реализациями поточных шифров, представленных на европейский конкурс eSTREAM (как генераторов псевдослучайных последовательностей, к которым предъявляются наиболее строгие требования как по быстродействию, так и по статистическим свойствам выходных последовательностей). В число рассмотренных алгоритмов вошли как победители конкурса eSTREAM в категории «поточные шифры, ориентированные на аппаратную реализацию» (Grain, MICKEY, Trivium), так и алгоритмы, включенные в международные криптографические стандарты (все тот же Trivium). Данные о производительности и эффективности аппаратных реализаций алгоритмов взяты из работ [29, 30]. Сравнение проводилось по двум показателям: абсолютному быстродействию, отражающему скорость выработки выходной последовательности на максимальной тактовой частоте, и приведенному быстродействию, показывающему скорость выработки выходной последовательности на частоте 100 МГц. Сравнение показало, что оба прототипа существенно (в несколько раз) превосходят аналоги по скорости выработки выходной последовательности (рис. 7).

Помимо быстродействия важную роль играет эффективность аппаратной реализации, которая выражается в быстродействии на единицу аппаратных ресурсов (для FPGA корпорации Altera такой единицей является логический элемент – LE). Сравнение эффективности аппаратной реализации представлено на рис. 8.

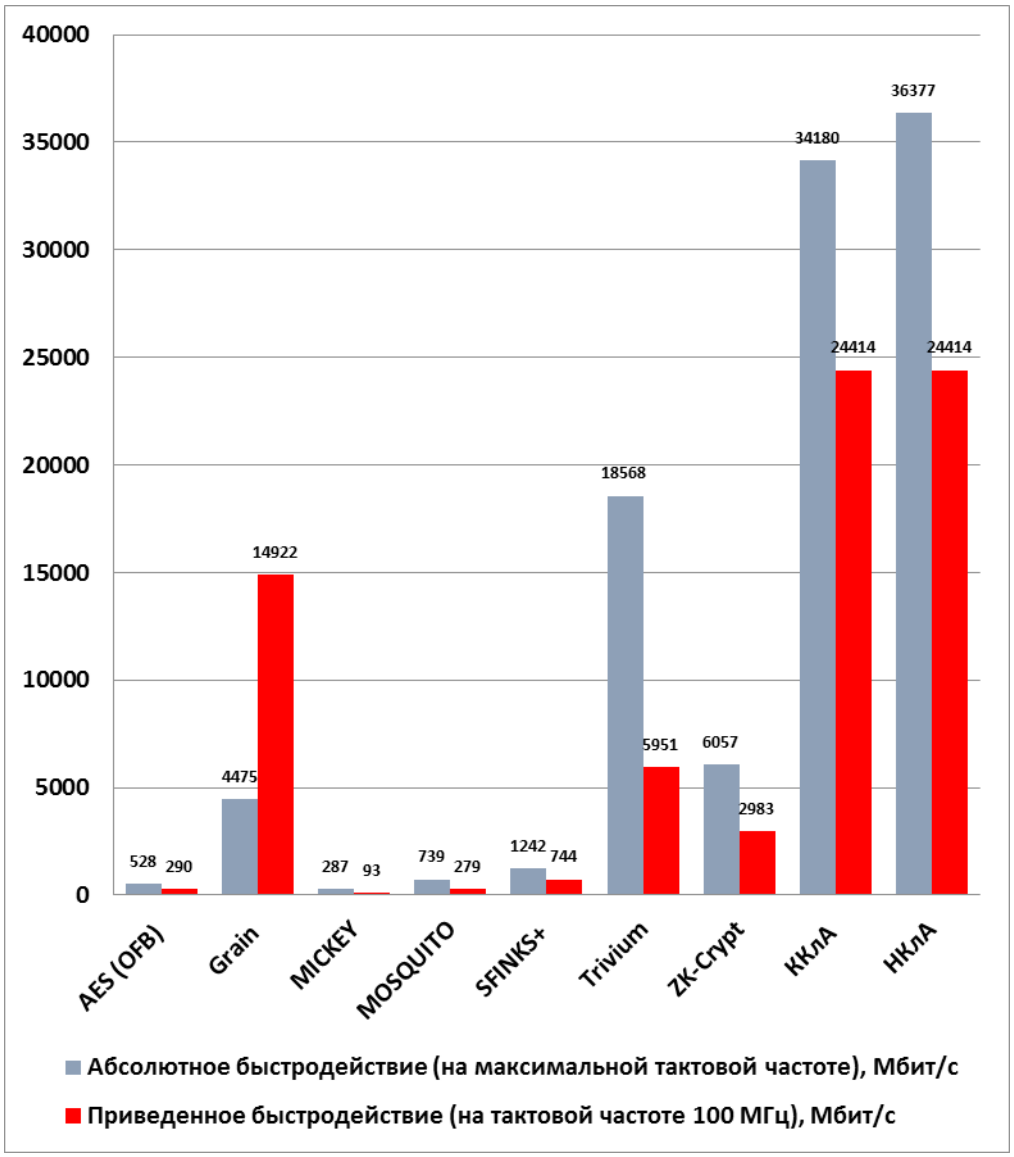


Рис. 7 *– Сравнение быстродействия разработанных аппаратных реализаций и некоторых существующих аналогов.*

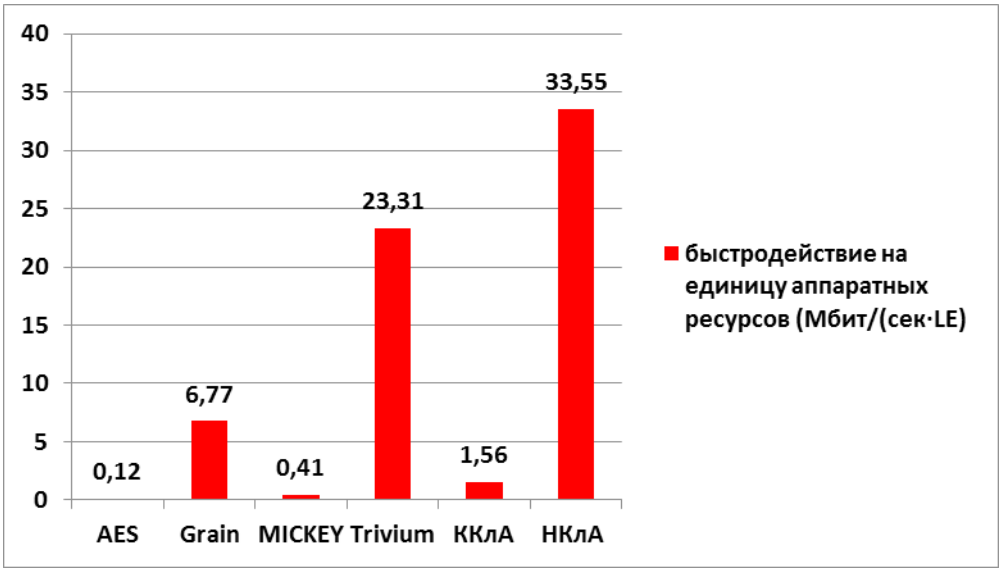


***Рис. 8** – Сравнение эффективности разработанных аппаратных реализаций и некоторых существующих аналогов.*

Из приведенных диаграмм видно, что по сравнению с другими алгоритмами аппаратная реализация генераторов НКлА является намного более эффективной и требует меньших аппаратных ресурсов FPGA. Эти показатели были достигнуты за счет использования обобщенных клеточных автоматов с локальной функцией связи от 4 переменных. В этом случае для реализации одной ячейки клеточного автомата потребуется всего 1 LE. Тем самым достигается оптимум по затрате логических элементов (LE) для данной микросхемы FPGA. Использование других моделей ПЛИС позволит с такой же эффективностью реализовывать обобщенные клеточные автоматы с локальной функцией связи от бóльшего числа переменных (что ведет к улучшению их криптографических свойств). Общий же вывод таков, что матрица LE является одной из наиболее удачных платформ для реализации алгоритмов на основе обобщенных клеточных автоматов.

В то же время следует отметить, что указанные конструкции предлагались исключительно в качестве генераторов псевдослучайных последовательностей и серьезный криптографический анализ предложенных ГПСП не проводился.

Клеточные автоматы в конструкции блочных шифров

Все попытки использовать клеточные автоматы в конструкции блочных шифров непосредственно в качестве цикловой функции шифрования упирались, прежде всего, в вопрос обратимости КлА.[8]) Если автомат является обратимым, обратное преобразование может быть реализовано также с помощью КлА (возможно с другой, в том числе и с бóльшей окрестностью по сравнению с исходным автоматом) [31].

Наиболее существенные результаты, связанные с вопросами обратимости, получены для классических КлА, заданных на бесконечных решетках. В работе [32] было показано, что для одномерных КлА задача алгоритмического распознавания обратимости является разрешимой. В той же работе был построен алгоритм распознавания, имеющий экспоненциальную сложность. Позже были построены алгоритмы для распознавания обратимости одномерных КлА, имеющие полиномиальную сложность [33-36]. Однако для клеточных автоматов на решетках с двумя и более измерениями таких алгоритмов нет. Было установлено [37, 38], что в общем случае эта задача является алгоритмически неразрешимой в том смысле, что не существует алгоритма, который для любого автомата всегда заканчивал бы свою работу в конечное время и давал бы правильный ответ. В работе [39] исследовались границы между классами клеточных автоматов, для которых свойство обратимости является алгоритмически разрешимым, и теми, для которых оно алгоритмически неразрешимо. Получен критерий разрешимости свойства обратимости для классов клеточных автоматов фиксированной размерности и с фиксированным числом состояний ячейки. Получен критерий разрешимости свойства обратимости в классе клеточных автоматов с фиксированной окрестностью (в терминологии автора [39] – с фиксированным шаблоном соседства).

8 КлА называется обратимым, если каждое его внутреннее состояние имеет единственный прообраз.

Построение обратимых КлА в случае размерностей, больших 1, весьма затруднительно. Известно несколько типов обратимых двумерных КлА, основными из которых являются блочные клеточные автоматы [17, 40] и клеточные автоматы второго порядка [41-43]. Автоматы этих типов отличаются от классических клеточных автоматов, однако доказано, что они могут быть эмулированы классическими клеточными автоматами (с, возможно, значительно бóльшим размером окрестности и числом состояний ячейки).

Для криптографических приложений, как правило, применяются КлА с решеткой конечного размера. Вопросы обратимости для таких КлА в принципе – всегда разрешимы, и основная задача состоит в нахождении приемлемых критериев для проверки обратимости, алгоритмов для реализации обратного преобразования и оценки сложности этих алгоритмов. В настоящее время эти вопросы весьма мало исследованы, результатов очень немного, а те какие есть – не внушают большого оптимизма на быстрое продвижение и скорые успехи в этом направлении. Так проводились попытки исследовать свойство обратимости двумерных КлА на множестве конфигураций, помещающихся в некоторый квадрат. В работе французского исследователя Б. Дюранда (Durand B.) было установлено, что задача распознавания обратимости в этой постановке является *co-NP*-полной [44].

В свою очередь, для обобщенных КлА, как показано в [45], задача восстановления предыдущего состояния (а значит и начального заполнения) обобщенного клеточного автомата является *NP*-трудной. Там же показано, что в случае КлА с локальной функцией связи от 2 переменных, задача о существовании предыдущего состояния принадлежит классу *P*.

Несмотря на отсутствие разработанной теории построения обратимых КлА с решеткой конечного размера, в последнее время предложено достаточно много блочных алгоритмов шифрования на основе обратимых КлА, в том числе и двумерных [46-53]. Кроме того, имеется значительное число работ, посвященных использованию КлА для построения S-блоков [54-59].

Наиболее же перспективным, по нашему мнению, является применение обобщенных КлА в алгоритмах блочного шифрования в качестве SPK-узла.

Концепция SPK-узла

При построении блочных шифров обычно применяются композиции преобразований, осуществляющих рассеивание и перемешивание преобразуемой информации, что достигается с помощью использования так называемых P-блоков (P-box) и S-блоков (S-box). При этом смешение с ключевой информацией, как правило, осуществляется или с помощью побитового сложения информационного блока с цикловым ключом, который вырабатывается из секретного ключа с помощью специального алгоритма, называемого алгоритмом выработки ключа, или (как, например, в алгоритме ГОСТ 28147-89) их сложения по модулю 2^n. Узел, осуществляющий смешение информационного блока с ключевой информацией, в дальнейшем будем называть K-блоком.

В поисках наиболее продуктивной реализации основных преобразований, задействованных в работе блочного шифра, была предложена концепция SPK-узла, то есть узла, который осуществляет некоторые нелинейные преобразования над входным информационным блоком и цикловым ключом, реализуя тем самым рассеивание и перемешивание, одновременно с этим осуществляя смешение информационного блока с ключевым материалом.

К одной из первых (во всяком случае, из опубликованных в открытой литературе) попыток создания такого узла можно отнести конструкцию Лая (Lai X.) и Месси (Massey J.), которая была применена в алгоритме блочного шифрования IDEA [60]. Авторами IDEA был предложен MA-узел (Multiplication-Addition), осуществляющий рассеивание, перемешивание и смешение с ключевым материалом входного информационного вектора. В алгоритме IDEA этот узел использовался в качестве цикловой функции шифрования.

MA-узел изображен на рис. 9. Здесь X_k – k-я часть входного информационного вектора, Y_k – k-я часть выходного информационного вектора, K_m – m-я часть циклового ключа, $\boxplus$ – операция сложения по модулю 2^{16}, $\otimes$ – операция умножения по модулю $2^{16}+1$. При этом конструкция данного алгоритма шифрования предполагает обратимость всех используемых операций (очевидно, это обстоятельство в основном касается операции умножения по модулю $2^{16}+1$). Хотя для указанных параметров обратимость операции умножения выполняется, ясно, что данный узел не годится для произвольного набора параметров, поскольку далеко не всегда число вида 2^k+1 является простым (простота модуля является необходимым и достаточным условием обратимости модульного умножения).

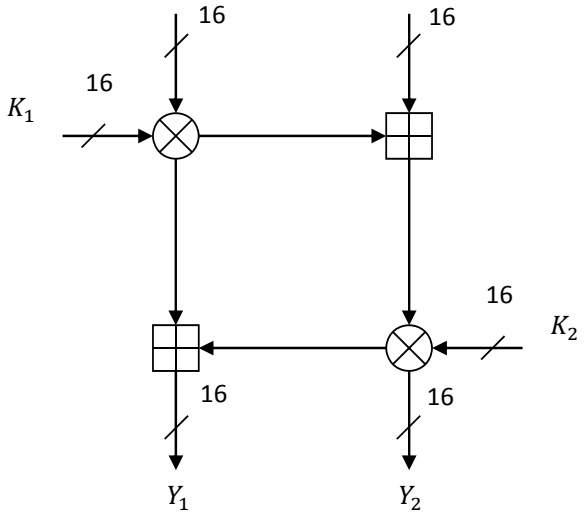


***Рис. 9** – Пример SPK-узла в алгоритме IDEA.*

Будем называть узлы данного типа SPK-узлами, так как они выполняют ту же функцию, что и композиции классических S-блоков и P-блоков с операцией сложения с цикловым ключом, которую мы договорились называть K-блоком.

Особо отметим, что в случае блочных шифров, имеющих структуру схемы Фейстеля, не требуется обратимость преобразований, входящих в состав шифрующей функции f (см. рис. 10, где l_i, r_i – части информационного блока, k_i – цикловой ключ, f – шифрующая функция).

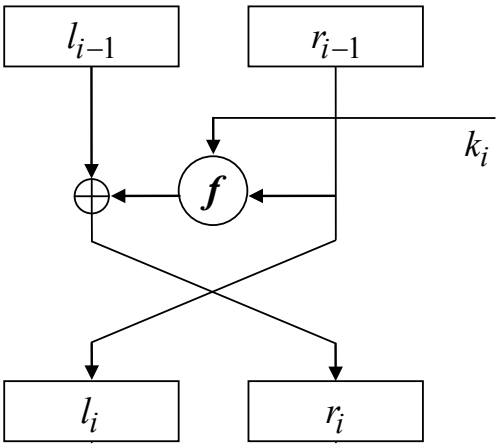


***Рис. 10** – Классическое преобразование Фейстеля.*

SPK-узлы на базе клеточных автоматов

Отличным кандидатом на применение в качестве SPK-узла являются обобщенные клеточные автоматы. SPK-узел – предложенный автором потенциально перспективный узел для включения в номенклатуру элементов, которые могут использоваться для построения алгоритмов блочного шифрования. Данный подход был впервые использован Балком Е.А. и развит Ключаревым П.Г. [27] в рамках исследований, проводимых на кафедре ИУ-8 МГТУ им.Н.Э.Баумана под руководством автора.

Пусть имеется однородный обобщенный клеточный автомат CA, задаваемый регулярным ориентированным графом $G = (V, E)$ где $V = \{v_1, v_2, \ldots, v_N\}$ – множество вершин, E – множество дуг, причем все вершины имеют полустепень захода равную δ. Пусть при этом диаметр графа равен d (далее будем называть δ – степенью захода обобщенного КлА, а d – диаметром обобщенного КлА). Тогда SPK-узлом на базе обобщенного КлА будем называть обобщенный клеточный автомат CA, начальное заполнение ячеек которого представляет собой n бит информационного вектора X и k бит ключевой информации K, $N = n + k$, осуществляющий преобразование $X \times K \to Y$. В рамках проведенных исследований размер выходного вектора Y выбирался равным размеру входного информационного вектора (рис. 11).

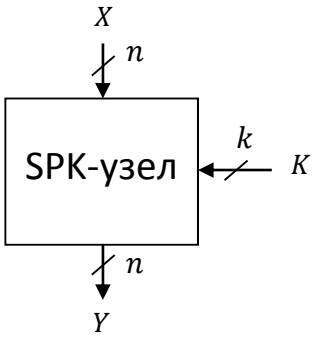


***Рис. 11** – Схема SPK-узла*

Таким образом, результатом преобразования SPK-узла на базе обобщенного клеточного автомата будет результат эволюции этого автомата, в процессе которой будет осуществлено и смешение с ключевым материалом, и перемешивание и рассеивание входной информации. При этом для обеспечения хорошего рассеивания и перемешивания минимальное число тактов работы автомата должно быть не меньше, чем d – диаметр графа, задающего этот автомат.

Число переменных, от которых должна существенно зависеть локальная функция связи, должно быть равным δ – степени захода обобщенного КлА. Преимуществом данного SPK-узла является то, что на каждом такте работы обобщенного КлА значение каждой вершины зависит от значения других вершин на предыдущем такте. Следовательно, вычисление ее нового состояния никак не

связано с вычислением состояния других вершин. Последнее означает, что новое состояние каждой вершины можно вычислять параллельно с вычислением состояний остальных вершин. Это дает существенное преимущество в применении данных узлов в алгоритмах, реализуемых на платформах, где имеется возможность распараллеливать вычисления.

Принципы построения клеточных автоматов

Для построения надежного алгоритма блочного шифрования на базе клеточных автоматов необходимо правильно выбрать сам клеточный автомат. Обобщенный КлА полностью задается следующими параметрами, которые требуется выбрать разработчику:

- структура графа;
- локальная функция связи.

Рассмотрим каждый параметр отдельно.

Выбор структуры графа

Выбор структуры графа имеет значение для криптостойкости алгоритма. В работе [28] автором предлагается набор требований, предъявляемых к неориентированному графу, используемому для задания структуры обобщенного клеточного автомата:

1. Граф должен иметь хаотическую структуру;
2. Диаметр графа должен быть мал;
3. Граф должен быть регулярным;
4. Граф не должен иметь петель и кратных ребер;

В исследованиях, проведенных Бардышевым А.А., Бородиным А.А., Грозмани Н.Ю.[9], использовались ориентированные графы, которые удовлетворяли условиям, описанным выше. Кроме того, в связи с ориентированностью используемых графов, появились как уточняющие, так и дополнительные условия:

1. Граф не должен иметь параллельных и антипараллельных дуг. Т.е. если множество E всех дуг графа содержит дугу (u,v), то это единственная дуга, соединяющая указанные вершины;

2. Все вершины должны иметь одну и ту же полустепень захода и полустепень исхода, т.е. граф должен быть сильно регулярным.

Одним из важных направлений исследования является анализ зависимости (или отсутствия таковой) сложности реализации клеточного автомата от размера графа, определяющего этот автомат, структуры этого графа и от значения полустепени захода/исхода.

Выбор локальной функции связи

Не менее важным является правильный выбор локальной функции связи обобщенного клеточного автомата. Булева функция f_i, ассоциированная с каждой из вершин графа автомата, должна удовлетворять условиям, усложняющим криптоанализ алгоритма.

В результате исследований [15, 28] был предложен ряд условий:

1. Функция должна существенно зависеть от всех своих аргументов.
2. Функция должна быть равновесной.
3. Нелинейность функции[10]) должна быть максимально большой, при соблюдении в то же время остальных наложенных на нее условий.

Одной из исследовательских задач является изучение зависимости сложности реализации от выбора локальной функции связи.

Для оценки эффективности реализации разработанных на базе SPK-узла симметрических блочных алгоритмов BCAF и BCNS, Грозмани Н.Ю. было осуществлено сравнение этих алгоритмов с классическими блочными алгоритмами шифрования – алгоритмом ГОСТ 28147-89 в режиме простой замены и алгоритмом PRESENT. Алгоритм ГОСТ выбран как российский стандарт симметричного шифрования, допускающий низкоресурсную реализацию [60, 61], а PRESENT – как принятый международный стандарт для низкоресурсной криптографии [62-64]. Параметры алгоритмов BCAF и BCNS были выбраны такими же, как и у алгоритма PRESENT: информационный блок – 64 бита, длина ключа – 80 бит.

Для аппаратной реализации указанных алгоритмов была выбрана микросхема ПЛИС Cyclone II EP2C50F484C6, обладающая всеми необходимыми параметрами и обеспечивающая высокое быстродействие по приемлемой цене. Языком программирования аппаратуры был выбран VHDL. По результатам реализации были получены данные о требуемом числе логических элементов и о быстродействии алгоритмов. Данные проведенных экспериментов приведены на рис. 12, 13.

В результате этого и на основании еще целого ряда проведенных исследований можно утверждать, что при использовании параллельных вычислительных устройств реализации блочных шифров, использующих SPK-узлы на основе обобщенных КлА, являются более эффективными, чем реализации шифров, использующих классические

9 Кафедра ИУ-8 МГТУ им.Н.Э.Баумана

10 Под нелинейностью булевой функции понимается расстояние (в метрике Хэмминга) от нее до множества аффинных функций.

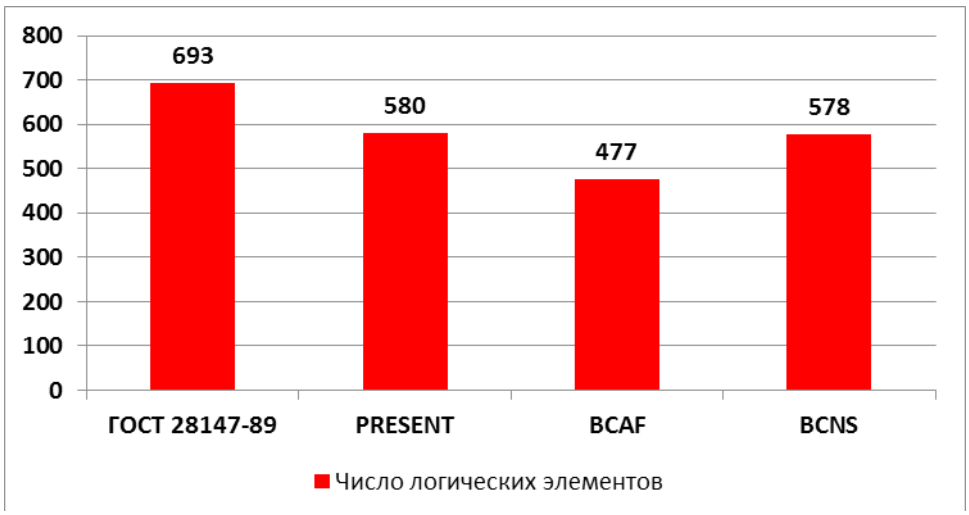


***Рис. 12** – Количество логических элементов в реализации алгоритмов блочного шифрования*

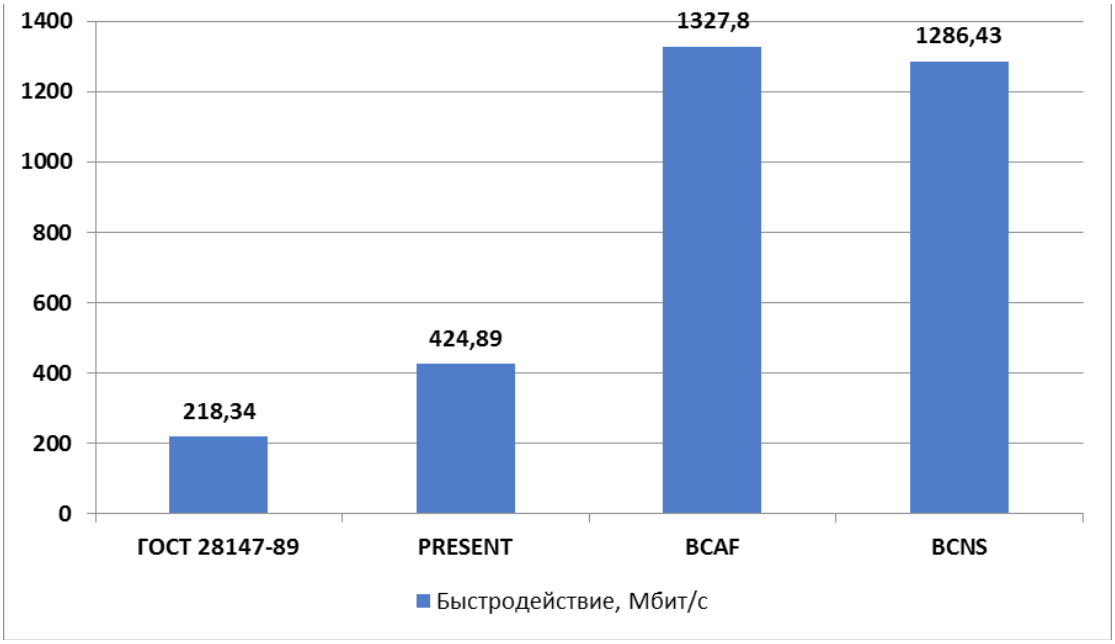


***Рис. 13** – Скоростные характеристики реализаций алгоритмов блочного шифрования*

S-, P-, K-блоки, вне зависимости от архитектуры построения шифра: легковесной или производительной.

Клеточный автомат в качестве цикловой шифрующей функции обобщенной схемы Фейстеля

В блочных шифрах, имеющих структуру классической схемы Фейстеля, в которых использовался SPK-узел на основе КлА [27], размерность входных данных SPK-узла (т.е. данных, образующих начальное заполнение КлА) превосходит размерность выхода. Таким образом, можно сказать, что часть вычислений, произведенных клеточным автоматом, не участвует в преобразовании информационного блока и как бы «пропадает даром». Ставя целью наибольшую продуктивность реализации преобразований, участвующих в работе блочного шифра, можно предложить следующую схему.

Пусть размер информационного блока блочного шифра равен $(t+1)\cdot m$ бит. Рассмотрим обобщенный клеточный автомат CA, структура которого задается орграфом $G(V,E)$ с N вершинами, $N = t \cdot m$. Пусть при этом в графе имеется независимое подмножество вершин[11]) мощности m. Клеточный автомат CA функционирует в качестве

11 Независимым будем называть такое подмножество вершин орграфа, что расстояние между любыми двумя вершинами из этого подмножества больше 1. Аналогично, независимым подмножеством 2-го порядка будем называть такое подмножество вершин, что расстояние между любыми двумя вершинами из этого подмножества больше 2.

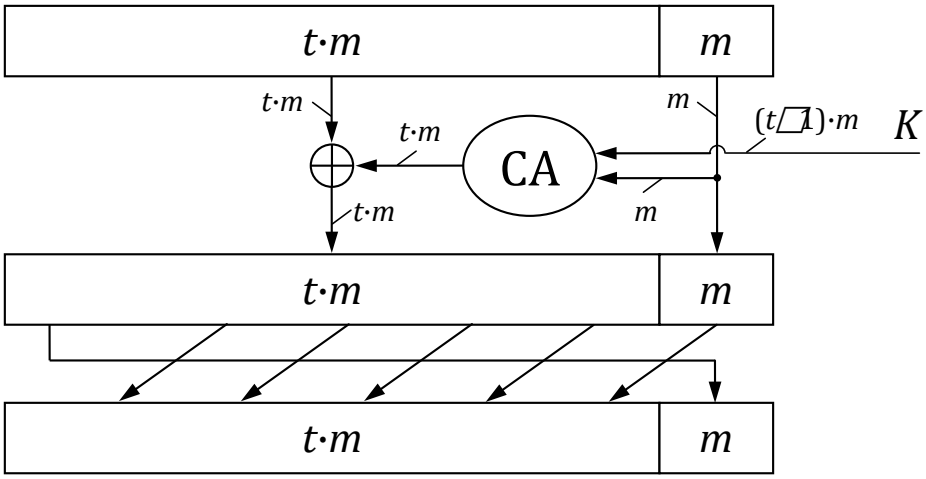


***Рис. 14** – Обобщенная схема Фейстеля с клеточным автоматом в качестве цикловой шифрующей функции*

шифрующей функции обобщенной схемы Фейстеля [65, 66]. Происходит это следующим образом:

- в m ячеек, соответствующих независимому подмножеству вершин графа клеточного автомата, загружается содержимое последних m битов информационного блока;
- в остальные $(t-1)\cdot m$ ячеек клеточного автомата загружается цикловой ключ *K*;
- клеточный автомат работает d тактов, где d – диаметр графа клеточного автомата;
- содержимое всех $N = t \cdot m$ ячеек клеточного автомата складывается с первыми $t \cdot m$ битами информационного блока.

После чего информационный блок циклически сдвигается на m разрядов (см. рис. 13).

Выбор независимого множества для загрузки битов информационного блока обусловлен исследованиями Бородина А.А., которые показали, что если в обобщенном КлА, используемом в блочном шифре в качестве SPK-узла, можно выбирать заполнение ячеек, соответствующих смежным вершинам графа, то на шифр можно провести атаку по выбранному открытому тексту (chosen plaintext attack). Подобные меры противодействия можно даже усилить, выбирая для записи битов информационного блока вершины, образующие независимое подмножество 2-го порядка. В этой связи появляется целый ряд задач, связанный с соответствующими свойствами ориентированных графов.

Как уже упоминалось выше, использование КлА в равновесных схемах Фейстеля – не вполне экономично, т.к. часть вычислений, проделанных в КлА, не участвует в преобразовании информационного блока. В этом смысле предлагаемый подход более продуктивен – результат *всех* вычислений, проделанных в КлА, используется в выработке шифртекста. Проведенные исследования также показывают, что для таких конструкций рассеивание и перемешивание информации происходит существенно быстрее, чем при использовании классических S-, P- и K-блоков. Однако, для того, чтобы предлагать SPK-узлы как актуальную замену классическим S-, P-, K-блокам требуется проведение более глубокого криптографического анализа предложенной конструкции, что становится важнейшей задачей ближайшего будущего.

Другие криптографические примитивы на базе клеточных автоматов

В довершение следует упомянуть, что клеточные автоматы по самóй своей природе весьма подходят для использования в конструкциях хэш-функций, кодов обнаружения модификации информации (MDC – Modification Detection Code) и кодов проверки подлинности сообщения (MAC – Message Authentication Code). В этом направлении предложено достаточно много конструкций. Так в работах [67-71] предлагаются различные конструкции хэш-функций, базирующиеся на использовании клеточных автоматов.

Что касается криптосистем с открытым ключом на базе клеточных автоматов, то их известно очень немного. Еще в 1987 году Гуань (Guan P.) предложил свою криптосистему [72], стойкость которой базируется на трудности решения системы нелинейных уравнений, что является *NP*-полной задачей. Задача обратимости многомерных клеточных автоматов лежит в основе стойкости другой криптосистемы с открытым ключом, предложенной Кари (Kari J.) [73] и получившей дальнейшее развитие в [74]. Еще одна криптосистема с открытым

ключом на базе клеточных автоматов была предложена в работе [75], однако она оказалась нестойкой по отношению к атакам по выбранному открытому тексту. Этих недостатков лишена схема, предложенная в [76].

Заключения

Подводя итоги, отметим, что клеточные автоматы привлекают все большее внимание криптографического сообщества в связи с тем, что распараллеленность их структуры позволяет увеличивать скорость работы и пропускную способность аппаратных реализаций криптоалгоритмов [68, 77]. Интересные перспективы появляются также при использовании КлА для построения криптографических алгоритмов, не требовательных к вычислительным ресурсам [63, 64, 78].

Особо следует сказать о перспективах использования клеточных автоматов в асимметричной криптографии. На сегодняшний день известно сравнительно небольшое число криптосистем с открытым ключом, причём к ним зачастую предъявляются претензии, как ввиду их малой скорости работы, так и по поводу недостаточного обоснования их стойкости. Вплоть до самого последнего времени «технологическая база» криптографии с открытым ключом продолжала оставаться чрезвычайно бедной. В основании стойкости таких систем обычно лежит вычислительная трудность решения некоторой задачи для какой-то алгебраической системы, чаще всего – алгебраической системы с элементами числовой природы. В подавляющем большинстве случаев это или задача факторизации больших чисел, или задача дискретного логарифмирования в циклической группе, чаще всего – мультипликативной группе конечного поля. Учитывая тот факт, что числа, как наиболее древние математические объекты, давно изучаются, неудивительны большие достижения в разработке алгоритмов для решения этих задач. В случае очередного успеха в этой области, системы, стойкость которых основана на задачах факторизации и вычисления дискретных логарифмов, могут стать значительно более уязвимыми или даже совершенно нестойкими. Еще более печальны перспективы указанных криптосистем в случае появления квантового компьютера, работающего с тысячами кубит (модели квантовых компьютеров, имеющиеся в настоящее время, работают с единицами кубит). Поиск же других алгебраических систем, применимых в криптографии с открытым ключом в постквантовом мире, является трудной задачей и требует вовлечения в криптографический обиход новых математических объектов [79]. В этой связи стоит обратить особое внимание на клеточные автоматы, которые представляют собой некоммутативные алгебраические структуры [80, 81], и более тщательно изучить вопросы их возможного использования в асимметричной криптографии.

Благодарности

Автор выражает свою признательность Б.М.Сухинину за полезные замечания, сделанные им в процессе обсуждения настоящей работы.

***Рецензент**: Цирлов Валентин Леонидович, доцент кафедры ИУ-8 МГТУ им.Н.Э.Баумана, v.tsirlov@bmstu.ru*

Литература:

1. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1. // Вопросы кибербезопасности. 2017. № 3 (21). С. 70-76.
2. Wolfram S. Theory and applications of cellular automata: Including selected papers 1983-1986. – River Edge, NJ.: World Scientific Publishing Co., Inc., 1986.
3. Wolfram S. Cryptography with Cellular Automata // Advances in Cryptology: Crypto '85 Proceedings. – Lecture Notes in Computer Science, vol. 218, 1986, pp. 429–432.
4. Meier W., Staffelbach O. Analysis of pseudo random sequences generated by cellular automata // Advances in Cryptology - EUROCRYPT ‹91 Proceedings. – Springer-Verlag, 1991, pp. 186–199.
5. Bardell P.H. Analysis of cellular automata used as pseudorandom pattern generators // Proceedings of 1990 International Test Conference, pp. 762–768.
6. Koc C.K., Apohan A.M. Inversion of cellular automata iteration // IEE Proceedings of Computer and Digital Technique. 1997, vol. 144, No. 5, pp. 279–284.
7. Blackburn S., Murphy S., Paterson K. Comments on theory and application of cellular automata in cryptography // IEEE Transactions on Computers. – 1997, vol. 46, No. 5, pp. 637–638.
8. Bao F. Cryptanalysys of a partially known cellular automata cryptosystem // IEEE Transactions on Computers. – 2004, vol. 53, No. 11, pp. 1493–1497.
9. Tomassini M., Sipper M. On the Generation of High-quality Random Numbers by Two-dimensional Cellular Automata // IEEE Trans. on Computers. – 2000, vol. 49. No 10, pp. 1140–1151.
10. Mohsen M. et al. Design of reconfigurable image encryption processor using 2-D cellular automata generator // International Journal of Computer Science and Applications. – 2009, vol. 6, No 4, pp. 43–62.

11. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование: электронное научно-техническое издание. – 2010. – № 9. С. 8.
12. Сухинин Б.М. О влиянии параметров локальной функции связи на распределение значений ячеек двоичных клеточных автоматов // Объединенный научный журнал. – 2010. – № 8. – С. 39–41.
13. Сухинин Б.М. О лавинном эффекте в клеточных автоматах // Объединенный научный журнал. – 2010. – №8. – С. 41–46.
14. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. – 2010. – №2. – С. 34–41.
15. Сухинин Б.М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование: электронное научно-техническое издание. – 2010. – №8. С. 1.
16. Feistel H. Cryprography and computer privacy. Scientific American. 1973, vol. 228, pp. 15–23.
17. Toffoli T., Margolus N. Cellular automata machines: A new environment for modeling. – Cambridge, Mass.: MIT Press, 1987.
18. Kauffman S.A. Metabolic stability and epigenesis in randomly constructed genetic nets // J. Theor. Biol. – 1969, No 22, pp. 437–467.
19. Gershenson C. Introduction to random boolean networks // Bedau M., Husbands P., Hutton T., Kumar S., Suzuki H. (eds.) Proceedings of the Workshops and Tutorials of the Ninth International Conference on the Simulation and Synthesis of Living Systems (ALife IX). – Boston, 2004, pp. 160–173.
20. Kauffman S.A. Behavior of randomly constructed genetics nets: Binary element nets // Waddington C.H. (ed.) Towards a Theoretical Biology. – Edinburgh University Press, 1970, pp. 18–37.
21. Kauffman S.A. Emergent properties in random complex automata // Physica D. – 1984, No 10, pp. 145–156.
22. Luczak T., Cohen J.E. Stability of vertices in random boolean cellular automata // Random Structures and Algorithms. – 1991, No 2, pp. 327–334.
23. Lynch J.F. A criterion for stability in random Boolean cellular automata // Ulam Quart. – 1993, No 2, pp. 32–44.
24. Lynch J.F. On the threshold of chaos in random Boolean cellular automata // Random Structures and Algorithms. – 1995, No 6, pp. 239–260.
25. Lynch J.F. Critical points for random Boolean networks // Physica D. – 2002, No 172, pp. 49–64.
26. Ключарёв П.Г. Клеточные автоматы, основанные на графах Рамануджана в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. – 2011. – № 10. С.22.
27. Ключарёв П.Г. Блочные шифры, основанные на обобщенных клеточных автоматах // Наука и образование. Электронное научно-техническое издание. – 2012. – №1. С.11.
28. Ключарёв П.Г. Построение псевдослучайных функций на основе обобщенных клеточных автоматов // Наука и образование. Электронное научно-техническое издание. – 2012. – №10. С.20.
29. Rogawski M. Hardware evaluation of eSTREAM candidates: Grain, Lex, Mickey128, Salsa20 and Trivium // The eSTREAM Project. – 2007. – 10 p.
30. Gurkaynak F. et al. Hardware evaluation of eSTREAM candidates: Achterbahn, Grain, MICKEY, MOSQUITO, SFINKS, Trivium, VEST, ZK-crypt // The eSTREAM Project. – 2006. – 12 p.
31. Richardson D. Tesselations with local transformations. Journal of Computer and System Sciences. – 1972, No 6, pp. 373–388.
32. Amoroso S., Patt Y.N. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures // J. Comput. System Sci. – 1972, No 6, № 5, pp. 448–464.
33. Sutner K. De Bruijn graphs and linear cellular automata // Complex Systems. – 1991, No 5(1), pp. 19–30.
34. Sutner K. Linear cellular automata and de Bruijn automata // Delorme M., Mazoyer J. (eds.) Cellular Automata: a parallel model. – Kluwer, 1998, pp. 303–319.
35. Culik K. On invertible cellular automata // Complex Systems. – 1987, No 1(6), pp. 1035–1044.
36. Hillman D. The structure of reversible one-dimensional cellular automata // Physica D: Nonlinear Phenomena. – 1991, No 52 (2-3), pp. 277–292.
37. Kari J. Reversibility of 2D cellular automata is undecidable // Physica D. – 1990, No 45, pp. 379–385.
38. Kari J. Reversibility and surjectivity problems of cellular automata // Journal of Computer and System Science. – 1994, No 48(1), pp. 149–182.
39. Кучеренко И.В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы. – 2004, No 8, №1-4. С. 465–482.
40. Schiff J.L. Cellular automata. A Discrete View of the World. – A John Wiley & Sons Inc., Publication. University of Auckland.– 2008.– 279 p.
41. Margolus N. Physics-like models of computation // Physica D: Nonlinear Phenomena. – 1984, No 10, pp. 81–95.
42. Vichniac G. Simulating physics with cellular automata // Physica D: Nonlinear Phenomena. – 1984, No 10, pp. 96–115.
43. Wolfram S. Cellular Automata as Models of Complexity // Nature. – 1984, No 311, pp. 419–424.
44. Durand B. Inversion of 2D cellular automata: some complexity results // Theoretical Computer Science. – 1994, vol. 134, No 2, pp. 387–401.
45. Ключарёв П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. Электронное научно-техническое издание. – 2012. – №1.
46. Anghelescu P., EmilSofron S. Block Encryption Using Hybrid Additive Cellular Automata // Proc. of 7-th International Conference on Hybrid Intelligent Systems. – 2007, pp. 132–137.
47. Kumar J.K.J. et al. Improving Resistance against Attack of L2DCASKE Encryption Algorithm by using RCA Rule 30 based S-Box // International Journal of Computer Applications. – 2013, vol. 70, No16, pp. 26–30.
48. Peridier V.J. Basic schemes for reversible two-dimensional cellular automata // Complex Systems. – 2008. – 18, pp. 44–51.

49. Seredynski F., Pienkosz K., Bouvry P. Reversible cellular automata based encryption // NPC'04, Lecture Notes in Computer Science, vol. 3222. – Springer-Verlag, 2004. – pp. 411–418.
50. Seredynski F., Bouvry P. Block Encryption Using Reversible Cellular Automata // Proceedings of ACRI 2004, Lecture Notes in Computer Science, vol. 3305. – Springer-Verlag, 2004, pp. 785–792.
51. Tripathy S., Nandi S. LCASE – Lightweight Cellular Automata-based Symmetric-key Encryption // International Journal of Network Security. – 2009, vol. 8, № 2. – pp.243–252.
52. Wells R.D. An analysis of cellular automata in cipher systems. – University of London, 2012.
53. Xia X., Li Y., Xia Z., Wang R. Data Encryption Based on Multi-Granularity Reversible Cellular Automata // Proc. of International Conference on Computational Intelligence and Security. – 2009, pp. 192–196.
54. Bhattacharya D., Bansal N., Banerjee A., RoyChowdhury D. A Near Optimal S-Box Design // ICISS 2007. – Lecture Notes in Computer Science, vol. 4812. – Springer-Verlag, 2007, pp. 77–90.
55. Szaban, M., Seredynski, F.: Cryptographically Strong S-Boxes Based on Cellular Automata // ACRI 2008. – Lecture Notes in Computer Science, vol. 5191. – Springer-Verlag, 2008, pp. 478–485.
56. Szaban M., Nowacki J.P., Drabik A., Seredynski F., Bouvry P. Application of Cellular Automata in Symmetric Key Cryptography // IAIT 2010, CCIS 114. – 2010, pp. 154–163.
57. Szaban M., Seredynski F. Properties of Safe Cellular Automata-Based S-Boxes // PPAM 2009, Part II. – Lecture Notes in Computer Science, vol. 6068. – Springer-Verlag, 2010. – Springer-Verlag, pp. 585–592.
58. Szaban M., Seredynski F. Improving quality of DES S-boxes by cellular automata-based S-boxes // J. Supercomput. – 2011. – 57, pp. 216–226
59. Szaban M., Seredynski F. Dynamic Cellular Automata-Based S-Boxes // EUROCAST 2011, Part I. – Lecture Notes in Computer Science, vol. 6927. – Springer-Verlag, 2012, pp. 184–191.
60. Lai X., Massey J. A Proposal for a New Block Encryption Standard // Advances in Cryptology: EUROCRYPT 1990 Proceedings. – Lecture Notes in Computer Science, vol. 473. – Springer-Verlag, 1991, pp. 389–404.
61. Poschmann A., Ling S., Wang H. 256 Bit Standardized Crypto for 650 GE – GOST Revisited // CHES 2010, LNCS 6225, pp. 219–233, 2010.
62. Dmukh A.A., Dygin D.M., Marshalko G.B. A lightweightfriendly modification of GOST block cipher // Математические вопросы криптографии. – 2014. – Т. 5, № 2. – с. 47–55.
63. Жуков А.Е. Легковесная криптография. Часть 1. // Вопросы кибербезопасности. 2015. № 1 (9). С. 26-43.
64. Жуков А.Е. Легковесная криптография. Часть 2. // Вопросы кибербезопасности. 2015. № 2 (10). С. 2-10.
65. Schneier B., Kelsey J. Unbalanced Feistel networks and block-cipher design // Fast Software Encryption 1996. – Lecture Notes in Computer Science, vol. 1039. – Springer-Verlag, 1996, pp. 121–144.
66. Жуков А.Е. Математические модели криптографии // Защита информации. Инсайд. – 2011. – №5. – С. 78–83.
67. Daemen J., Govaerts R., Vandewalle J. A Framework for the Design of One-Way Hash Functions Including Cryptanalysis of Damgerd's One-Way Function Based on a Cellular Automaton // Advances in Cryptology – Proceedings of ASIACRYPT ‹91. – Lecture Notes in Computer Science, vol. 739. – Springer-Verlag, 1993, pp. 82–96.
68. Mihaljevic M.J., Zheng Y., Imai H. A Cellular Automaton Based Fast One-Way Hash Function Suitable for Hardware Implementation // Proceedings of Public Key Cryptography ‹98. – Lecture Notes in Computer Science, vol. 1431. – Springer-Verlag, 1998, pp. 217–233.
69. Yoon J.W., Shin S.U., Rhee K.H. A secure hash function based on cellular automata // Proceedings of the 1-st International Conference on Information Security and Cryptology ‹98. – Korea Institute of Information Security and Cryptology (KIISC), 1998, pp. 93–105.
70. Ключарёв П.Г. Криптографические хэш-функции, основанные на обобщенных клеточных автоматах // Наука и образование. Электронное научно-техническое издание. – 2013. – №1.
71. Ключарёв П.Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. 2017. № 1 (19). С. 45-50.
72. Guan P. Cellular automaton public-key cryptosystems // Complex Systems. – 1987, vol. 1, pp. 51–57.
73. Kari J. Cryptosystems based on reversible cellular automata. Tech. rep. – Finland, University of Turku, 1992.
74. Clarridge A., Salomaa K. A cryptosystem based on the composition of reversible cellular automata // LATA'2009, Lecture Notes in Computer Science, vol. 5457. – 2009, pp. 314–325.
75. Zhu B., Zhou L. Public key cryptosystem based on cellular automata // Journal of Nanjing University of Science and Technology. – 2007.
76. Zhang X., Lu R., Zhang H., Xu C. A New Public Key Encryption Scheme based on Layered Cellular Automata // KSII Transactions on Internet and Information Systems. – 2014, vol. 8, № 10, pp. 3572–3590
77. Franti E., Slav C., Balan T. Design of Cellular Automata Hardware for Cryptographic Application // Proc. of CAS'2004 Int. Semiconductor Conference. – 2004. – 2, pp. 463–466.
78. Жуков А.Е. Низкоресурсная криптография: актуальность, востребованность, основные требования и подходы. – Защита информации. Инсайд. 2015, №4, с. 20–31; №5, с. 71–81
79. Жуков А.Е. Криптография с открытым ключом и нечисловые алгебраические системы. – Безопасность информационных технологий. – 2003. – Вып. 1, с. 22–29.
80. Pedersen J. Cellular automata as algebraic systems // Complex Systems. – 1992. – 6, pp. 237–250.
81. Ceccherini-Silberstein T., Coornaert M. Cellular automata and groups // Springer Monographs in Mathematics. – Berlin: Springer-Verlag, 2010. – 439 p.

CELLULAR AUTOMATA IN CRYPTOGRAPHY. Part 2.

Zhukov A.E.[12]

Cellular automata are widespread and ubiquitous [1]. They are independent objects of theoretical study, as well as a modeling tool in science and technology. The popularity of cellular automata is based on their relative simplicity combined with numerous possibilities for modeling sets of interconnected homogeneous objects. Besides that, cellular automata, as parallel structures, are perfectly useful for modeling discrete parallel processes, for creating parallel algorithms for information processing and are also a basis of computer technology with a highly parallel architecture.

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

References:

1. ZHukov A.E. Kletochnye avtomaty v kriptografii. CHast' 1, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 3 (21). P. 70-76. DOI: 10.21581/2311-3456-2017-2-70-76.
2. Wolfram S. Theory and applications of cellular automata: Including selected papers 1983-1986. – River Edge, NJ.: World Scientific Publishing Co., Inc., 1986.
3. Wolfram S. Cryptography with Cellular Automata, Advances in Cryptology: Crypto '85 Proceedings. – Lecture Notes in Computer Science, vol. 218, 1986, pp. 429–432.
4. Meier W., Staffelbach O. Analysis of pseudo random sequences generated by cellular automata, Advances in Cryptology - EUROCRYPT ‹91 Proceedings. – Springer-Verlag, 1991, pp. 186–199.
5. Bardell P.H. Analysis of cellular automata used as pseudorandom pattern generators, Proceedings of 1990 International Test Conference, pp. 762–768.
6. Koc C.K., Apohan A.M. Inversion of cellular automata iteration, IEE Proceedings of Computer and Digital Technique. 1997, vol. 144, No. 5, pp. 279–284.
7. Blackburn S., Murphy S., Paterson K. Comments on theory and application of cellular automata in cryptography, IEEE Transactions on Computers. – 1997, vol. 46, No. 5, pp. 637–638.
8. Bao F. Cryptanalysys of a partially known cellular automata cryptosystem, IEEE Transactions on Computers. – 2004, vol. 53, No. 11, pp. 1493–1497.
9. Tomassini M., Sipper M. On the Generation of High-quality Random Numbers by Two-dimensional Cellular Automata, IEEE Trans. on Computers. – 2000, vol. 49. No 10, pp. 1140–1151.
10. Mohsen M. et al. Design of reconfigurable image encryption processor using 2-D cellular automata generator, International Journal of Computer Science and Applications. – 2009, vol. 6, No 4, pp. 43–62.
11. Suhinin B.M. Razrabotka generatorov psevdosluchajnyh dvoichnyh posledovatel'nostej na osnove kletochnyh avtomatov, Nauka i obrazovanie: ehlektronnoe nauchno-tekhnicheskoe izdanie. – 2010. – No 9. C. 8.
12. Suhinin B.M. O vliyanii parametrov lokal'noj funkcii svyazi na raspredelenie znachenij yacheek dvoichnyh kletochnyh avtomatov, Ob»edinennyj nauchnyj zhurnal. – 2010. – No 8. – S. 39–41.
13. Suhinin B.M. O lavinnom ehffekte v kletochnyh avtomatah, Ob»edinennyj nauchnyj zhurnal. – 2010. – No8. – S. 41–46.
14. Suhinin B.M. Vysokoskorostnye generatory psevdosluchajnyh posledovatel'nostej na osnove kletochnyh avtomatov, Prikladnaya diskretnaya matematika. – 2010. – No2. – S. 34–41.
15. Suhinin B.M. Issledovanie harakteristik lavinnogo ehffekta v dvoichnyh kletochnyh avtomatah s ravnovesnymi funkciyami perekhodov, Nauka i obrazovanie: ehlektronnoe nauchno-tekhnicheskoe izdanie. – 2010. – No8. C. 1.
16. Feistel H. Cryprography and computer privacy. Scientific American. 1973, vol. 228, pp. 15–23.
17. Toffoli T., Margolus N. Cellular automata machines: A new environment for modeling. – Cambridge, Mass.: MIT Press, 1987.
18. Kauffman S.A. Metabolic stability and epigenesis in randomly constructed genetic nets, J. Theor. Biol. – 1969, No 22, pp. 437–467.
19. Gershenson C. Introduction to random boolean networks, Bedau M., Husbands P., Hutton T., Kumar S., Suzuki H. (eds.) Proceedings of the Workshops and Tutorials of the Ninth International Conference on the Simulation and Synthesis of Living Systems (ALife IX). – Boston, 2004, pp. 160–173.
20. Kauffman S.A. Behavior of randomly constructed genetics nets: Binary element nets, Waddington C.H. (ed.) Towards a Theoretical Biology. – Edinburgh University Press, 1970, pp. 18–37.
21. Kauffman S.A. Emergent properties in random complex automata, Physica D. – 1984, No 10, pp. 145–156.
22. Luczak T., Cohen J.E. Stability of vertices in random boolean cellular automata, Random Structures and Algorithms. – 1991, No 2, pp. 327–334.
23. Lynch J.F. A criterion for stability in random Boolean cellular automata, Ulam Quart. – 1993, No 2, pp. 32–44.
24. Lynch J.F. On the threshold of chaos in random Boolean cellular automata, Random Structures and Algorithms. – 1995, No 6, pp. 239–260.
25. Lynch J.F. Critical points for random Boolean networks, Physica D. – 2002, No 172, pp. 49–64.

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

26. Klyucharyov P.G. Kletochnye avtomaty, osnovannye na grafah Ramanudzhana v zadachah generacii psevdosluchajnyh posledovatel'nostej, Nauka i obrazovanie. EHlektronnoe nauchno-tekhnicheskoe izdanie. – 2011. – No 10. S.22.
27. Klyucharyov P.G. Blochnye shifry, osnovannye na obobshchennyh kletochnyh avtomatah, Nauka i obrazovanie. EHlektronnoe nauchno-tekhnicheskoe izdanie. – 2012. – No 1. S.11.
28. Klyucharyov P.G. Postroenie psevdosluchajnyh funkcij na osnove obobshchennyh kletochnyh avtomatov, Nauka i obrazovanie. EHlektronnoe nauchno-tekhnicheskoe izdanie. – 2012. – No 10. S.20.
29. Rogawski M. Hardware evaluation of eSTREAM candidates: Grain, Lex, Mickey128, Salsa20 and Trivium, The eSTREAM Project. – 2007. – 10 p.
30. Gurkaynak F. et al. Hardware evaluation of eSTREAM candidates: Achterbahn, Grain, MICKEY, MOSQUITO, SFINKS, Trivium, VEST, ZK-crypt, The eSTREAM Project. – 2006. – 12 p.
31. Richardson D. Tesselations with local transformations. Journal of Computer and System Sciences. – 1972, No 6, pp. 373–388.
32. Amoroso S., Patt Y.N. Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures, J. Comput. System Sci. – 1972, No 6, No 5, pp. 448–464.
33. Sutner K. De Bruijn graphs and linear cellular automata, Complex Systems. – 1991, No 5(1), pp. 19–30.
34. Sutner K. Linear cellular automata and de Bruijn automata, Delorme M., Mazoyer J. (eds.) Cellular Automata: a parallel model. – Kluwer, 1998, pp. 303–319.
35. Culik K. On invertible cellular automata, Complex Systems. – 1987, No 1(6), pp. 1035–1044.
36. Hillman D. The structure of reversible one-dimensional cellular automata, Physica D: Nonlinear Phenomena. – 1991, No 52 (2-3), pp. 277–292.
37. Kari J. Reversibility of 2D cellular automata is undecidable, Physica D. – 1990, No 45, pp. 379–385.
38. Kari J. Reversibility and surjectivity problems of cellular automata, Journal of Computer and System Science. – 1994, No 48(1), pp. 149–182.
39. Kucherenko I.V. O razreshimosti obratimosti kletochnyh avtomatov, Intellektual'nye sistemy. – 2004, No 8, No1-4. C. 465–482.
40. Schiff J.L. Cellular automata. A Discrete View of the World. – A John Wiley & Sons Inc., Publication. University of Auckland.– 2008.– 279 p.
41. Margolus N. Physics-like models of computation, Physica D: Nonlinear Phenomena. – 1984, No 10, pp. 81–95.
42. Vichniac G. Simulating physics with cellular automata, Physica D: Nonlinear Phenomena. – 1984, No 10, pp. 96–115.
43. Wolfram S. Cellular Automata as Models of Complexity, Nature. – 1984, No 311, pp. 419–424.
44. Durand B. Inversion of 2D cellular automata: some complexity results, Theoretical Computer Science. – 1994, vol. 134, No 2, pp. 387–401.
45. Klyucharyov P.G. NP-trudnost' zadachi o vosstanovlenii predydushchego sostoyaniya obobshchennogo kletochnogo avtomata, Nauka i obrazovanie. EHlektronnoe nauchno-tekhnicheskoe izdanie. – 2012. – No1.
46. Anghelescu P., EmilSofron S. Block Encryption Using Hybrid Additive Cellular Automata, Proc. of 7-th International Conference on Hybrid Intelligent Systems. – 2007, pp. 132–137.
47. Kumar J.K.J. et al. Improving Resistance against Attack of L2DCASKE Encryption Algorithm by using RCA Rule 30 based S-Box, International Journal of Computer Applications. – 2013, vol. 70, No16, pp. 26–30.
48. Peridier V.J. Basic schemes for reversible two-dimensional cellular automata, Complex Systems. – 2008. – 18, pp. 44–51.
49. Seredynski F., Pienkosz K., Bouvry P. Reversible cellular automata based encryption, NPC'04, Lecture Notes in Computer Science, vol. 3222. – Springer-Verlag, 2004. – pp. 411–418.
50. Seredynski F., Bouvry P. Block Encryption Using Reversible Cellular Automata, Proceedings of ACRI 2004, Lecture Notes in Computer Science, vol. 3305. – Springer-Verlag, 2004, pp. 785–792.
51. Tripathy S., Nandi S. LCASE – Lightweight Cellular Automata-based Symmetric-key Encryption, International Journal of Network Security. – 2009, vol. 8, No 2. – pp.243–252.
52. Wells R.D. An analysis of cellular automata in cipher systems. – University of London, 2012.
53. Xia X., Li Y., Xia Z., Wang R. Data Encryption Based on Multi-Granularity Reversible Cellular Automata, Proc. of International Conference on Computational Intelligence and Security. – 2009, pp. 192–196.
54. Bhattacharya D., Bansal N., Banerjee A., RoyChowdhury D. A Near Optimal S-Box Design, ICISS 2007. – Lecture Notes in Computer Science, vol. 4812. – Springer-Verlag, 2007, pp. 77–90.
55. Szaban, M., Seredynski, F.: Cryptographically Strong S-Boxes Based on Cellular Automata, ACRI 2008. – Lecture Notes in Computer Science, vol. 5191. – Springer-Verlag, 2008, pp. 478–485.
56. Szaban M., Nowacki J.P., Drabik A., Seredynski F., Bouvry P. Application of Cellular Automata in Symmetric Key Cryptography, IAIT 2010, CCIS 114. – 2010, pp. 154–163.
57. Szaban M., Seredynski F. Properties of Safe Cellular Automata-Based S-Boxes, PPAM 2009, Part II. – Lecture Notes in Computer Science, vol. 6068. – Springer-Verlag, 2010. – Springer-Verlag, pp. 585–592.
58. Szaban M., Seredynski F. Improving quality of DES S-boxes by cellular automata-based S-boxes, J. Supercomput. – 2011. – 57, pp. 216–226
59. Szaban M., Seredynski F. Dynamic Cellular Automata-Based S-Boxes, EUROCAST 2011, Part I. – Lecture Notes in Computer Science, vol. 6927. – Springer-Verlag, 2012, pp. 184–191.
60. Lai X., Massey J. A Proposal for a New Block Encryption Standard, Advances in Cryptology: EUROCRYPT 1990 Proceedings. – Lecture Notes in Computer Science, vol. 473. – Springer-Verlag, 1991, pp. 389–404.
61. Poschmann A., Ling S., Wang H. 256 Bit Standardized Crypto for 650 GE – GOST Revisited, CHES 2010, LNCS 6225, pp. 219–233, 2010.
62. Dmukh A.A., Dygin D.M., Marshalko G.B. A lightweightfriendly modification of GOST block cipher, Matematicheskie voprosy kriptografii. – 2014. – T. 5, No 2. – c. 47–55.
63. ZHukov A.E. Legkovesnaya kriptografiya. CHast' 1, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015, No 1 (9). S. 26-43.
64. ZHukov A.E. Legkovesnaya kriptografiya. CHast' 2, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015, No 2 (10). S. 2-10.

65. Schneier B., Kelsey J. Unbalanced Feistel networks and block-cipher design, Fast Software Encryption 1996. – Lecture Notes in Computer Science, vol. 1039. – Springer-Verlag, 1996, pp. 121–144.
66. ZHukov A.E. Matematicheskie modeli kriptografii, Zashchita informacii. Insajd. – 2011. – No5. – S. 78–83.
67. Daemen J., Govaerts R., Vandewalle J. A Framework for the Design of One-Way Hash Functions Including Cryptanalysis of Damgerd's One-Way Function Based on a Cellular Automaton, Advances in Cryptology – Proceedings of ASIACRYPT ‹91. – Lecture Notes in Computer Science, vol. 739. – Springer-Verlag, 1993, pp. 82–96.
68. Mihaljevic M.J., Zheng Y., Imai H. A Cellular Automaton Based Fast One-Way Hash Function Suitable for Hardware Implementation, Proceedings of Public Key Cryptography ‹98. – Lecture Notes in Computer Science, vol. 1431. – Springer-Verlag, 1998, pp. 217–233.
69. Yoon J.W., Shin S.U., Rhee K.H. A secure hash function based on cellular automata, Proceedings of the 1-st International Conference on Information Security and Cryptology ‹98. – Korea Institute of Information Security and Cryptology (KIISC), 1998, pp. 93–105.
70. Klyucharyov P.G. Kriptograficheskie hehsh-funkcii, osnovannye na obobshchennyh kletochnyh avtomatah, Nauka i obrazovanie. EHlektronnoe nauchno-tekhnicheskoe izdanie. – 2013. – No1.
71. Klyucharyov P.G. Metod postroeniya kriptograficheskih hehsh-funkcij na osnove iteracij obobshchennogo kletochnogo avtomata, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 1 (19). P. 45-50. DOI: 10.21581/2311-3456-2017-1-45-50.
72. Guan P. Cellular automaton public-key cryptosystems, Complex Systems. – 1987, vol. 1, pp. 51–57.
73. Kari J. Cryptosystems based on reversible cellular automata. Tech. rep. – Finland, University of Turku, 1992.
74. Clarridge A., Salomaa K. A cryptosystem based on the composition of reversible cellular automata, LATA'2009, Lecture Notes in Computer Science, vol. 5457. – 2009, pp. 314–325.
75. Zhu B., Zhou L. Public key cryptosystem based on cellular automata, Journal of Nanjing University of Science and Technology. – 2007.
76. Zhang X., Lu R., Zhang H., Xu C. A New Public Key Encryption Scheme based on Layered Cellular Automata, KSII Transactions on Internet and Information Systems. – 2014, vol. 8, No 10, pp. 3572–3590
77. Franti E., Slav C., Balan T. Design of Cellular Automata Hardware for Cryptographic Application, Proc. of CAS'2004 Int. Semiconductor Conference. – 2004. – 2, pp. 463–466.
78. ZHukov A.E. Nizkoresursnaya kriptografiya: aktual'nost', vostrebovannost', osnovnye trebovaniya i podhody. – Zashchita informacii. Insajd.– 2015, No4, s. 20–31; No5, s. 71–81
79. ZHukov A.E. Kriptografiya s otkrytym klyuchom i nechislovye algebraicheskie sistemy. – Bezopasnost' informacionnyh tekhnologij. – 2003. – Vyp. 1, s. 22–29.
80. Pedersen J. Cellular automata as algebraic systems, Complex Systems. – 1992. – 6, pp. 237–250.
81. Ceccherini-Silberstein T., Coornaert M. Cellular automata and groups, Springer Monographs in Mathematics. – Berlin: Springer-Verlag, 2010. – 439 p.