УДК 621.391

О.О. Евсютин, С.К. Россошек

Использование клеточных автоматов для решения задач преобразования информации

Рассматривается возможность использования клеточных автоматов для решения задач преобразования информации, к которым относятся шифрование, кодирование и сжатие данных.

Ключевые слова: теория клеточных автоматов, моделирование, преобразование информации, информационная безопасность, криптография, сжатие данных.

В настоящее время выделяют два основных направления развития теории клеточных автоматов. Первым направлением является использование клеточных автоматов в качестве среды моделирования (симулирования) различных процессов, явлений и феноменов во многих областях науки. Второе направление рассматривает клеточные автоматы как самостоятельный объект исследования.

Среда, которую представляют собой клеточные автоматы, обладает большими возможностями для моделирования совокупности взаимосвязанных однородных объектов. Сюда можно отнести моделирование физических процессов в физике частиц и ядерной физике, моделирование движения потоков жидкости, моделирование взаимодействующих клеточных систем в биологии и медицине, использование моделей на основе клеточных автоматов в нанотехнологиях и т.д. Кроме того, клеточные автоматы являются по определению параллельными структурами и поэтому используются для решения проблем моделирования дискретных параллельных процессов, для создания параллельных алгоритмов обработки информации и представляют интерес в качестве основы вычислительной техники с высокопараллельной архитектурой [1].

Среди всего множества приложений теории клеточных автоматов можно выделить задачи преобразования информации, к которым, в свою очередь, можно отнести шифрование, кодирование и сжатие данных. Данный класс задач необходимо рассматривать отдельно, так как здесь в отличие от моделирования разного рода процессов, явлений и объектов смысл (физический или иной другой) преобразуемых данных не имеет значения. Это означает, что при решении некоторой задачи преобразования информации с помощью клеточного автомата основной интерес представляют поведенческие свойства выбранной клеточной структуры, в то время как при моделировании с помощью клеточных автоматов на первом месте стоят их структурные свойства.

В частности, при построении на основе клеточных автоматов алгоритма шифрования необходимо получить такую динамику развития клеточного автомата, которая позволит обеспечить криптографически безопасное шифрование, максимально устранив зависимость между входными и выходными данными.

Применение клеточных автоматов в криптографии дало на сегодняшний момент ряд результатов. Клеточные автоматы используются в однонаправленных функциях хэширования, в качестве генераторов псевдослучайных последовательностей, для шифрования информации [2, 6]. Кроме того, некоторые исследователи отмечают возможность построения криптосистемы с открытым ключом на основе клеточных автоматов, однако пока данная задача не нашла решения [3].

Общий подход к построению алгоритма шифрования на основе клеточных автоматов выглядит следующим образом.

Основой алгоритма является конечный клеточный автомат с решеткой некоторой размерности. Целесообразно выбирать одномерные, двумерные или трехмерные клеточные автоматы, поскольку в случае больших размерностей таблица правил будет громоздкой и неудобной в использовании.

Решетка конечного клеточного автомата содержит определенный объем информации, поэтому исходный (открытый) текст разбивается на блоки соответствующей длины, т.е. рассматриваемый алгоритм шифрования является блочным по определению.

Каждый блок открытого текста представляется в виде начального состояния решетки клеточного автомата, после чего клеточный автомат развивается во времени в течение заданного числа шагов. Развитие клеточного автомата, а соответственно и зашифрование, происходит под управлением секретного ключа, который напрямую в шифровании не участвует, а определяет таблицу правил клеточного автомата.

Такой подход предполагает, что клеточный автомат обладает свойством обратимости [4], позволяющим рассмотреть последовательность конфигураций клеточного автомата в обратном направлении, что делает возможным расшифрование зашифрованной информации. Однако возможно и использование необратимых клеточных автоматов в качестве вспомогательного элемента схемы шифрования.

О разработке и исследовании криптосистемы на основе обратимых клеточных автоматов на разбиении говорится в [5].

Другим перспективным, хотя и малоизученным, приложением теории клеточных автоматов является применение клеточных автоматов для сжатия данных.

Здесь возможны следующие направления исследований.

Во-первых, использование обратимых клеточных автоматов, если речь идет о сжатии без потерь. Если работа ведется с данными, допускающими потери, возможно использование необратимых клеточных автоматов. Вероятность успеха в этом случае, по-видимому, больше, поскольку среди всевозможных клеточных автоматов доля обратимых крайне мала.

Во-вторых, возможно комбинирование клеточных автоматов с уже существующими методами сжатия. В этом случае сжатие не будет осуществляться непосредственно с помощью клеточного автомата. С помощью обратимого клеточного автомата данные будут преобразованы таким образом, что их сжатие с помощью одного из существующих методов осуществится с большим эффектом.

Третий подход тесно связан с понятием конструируемости из теории клеточных автоматов. Он заключается в том, чтобы представить сжимаемые данные в виде состояния решетки клеточного автомата и попытаться определить путь от некоторого фиксированного состояния к данному. Тогда для восстановления сжатой информации нужно будет знать только порождающий алгоритм. Однако в общем случае определение такого алгоритма может оказаться достаточно трудной задачей.

Актуальность поиска новых способов сжатия информации с использованием клеточных автоматов определяется тем, что, несмотря на быстрое развитие средств вычислительной техники, проблема сокращения объема обрабатываемой, передаваемой и хранимой информации по-прежнему является важной, в особенности применительно к звуковой, фото- и видеоинформации [6].

Литература

1. Аладьев В.З. Классические однородные структуры. Теория и приложения / В.З. Аладьев, В.К. Бойко, Е.А. Ровба. – Гродно: ГрГУ, 2008. – 486 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – М.: Триумф, 2002. – 816 с.

3. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 318 с.

4. Тоффоли Т. Машины клеточных автоматов / Т. Тоффоли, Н. Марголус. – М.: Мир, 1991. – 280 с.

5. Евсютин О.О. Шифр на основе обратимых клеточных автоматов на разбиении / О.О. Евсютин, С.К. Росошек // Безопасность информационных технологий. – 2007. – № 4. – С. 27–31.

6. Криптографические протоколы в системах с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – № 12.1. – С. 51–61.

Евсютин Олег Олегович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: +7-923-403-09-21
Эл. адрес: eoo@keva.tusur.ru

Россошек Семен Константинович
Канд. физ.-мат. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: +7-952-803-87-80
Эл. адрес: rososhek@list.ru

O.O. Evsutin, S.K. Rososhek

Use of cellular automatons for problems solving of information transformation

Consider an availability use of cellular automatons for problems solving of information transformation, such as encryption, encoding and data compression.

Keywords: theory of cellular automatons, modeling, transformation of information, information security, cryptography, data compression.