23. *Gladkov L.A., Gladkova N.V., Leiba S.N., Strakhov N.E.* Development and research of the hybrid approach to the solution of optimization design problems, *Advances in Intelligent Systems and Computing. Vol. 875. International Conference on Intelligent Information Technologies for Industry IITI'18.* Springer Nature Switzerland AG, 2019, Vol. 2, pp. 246-257.
24. *Library Exchange Format.* University of Maryland, Baltimore County, 2011.
25. *Qt Documentation.* Available at: http://doc.qt.io/qt-5/reference-overview.html.

Статью рекомендовала к опубликованию д.т.н., профессор Л.С. Лисицына.

Ясир Муханад Джаббар Ясир – Южный федеральный университет; e-mail: yasir_82@mail.ru; г. Таганрог, Россия; тел.: 88634371625; кафедра САПР; аспирант.

Гладков Леонид Анатольевич – e-mail: lagladkov@sfedu.ru; тел.: 88634371625; кафедра САПР; к.т.н.; доцент.

Гладкова Надежда Викторовна – e-mail: nvgladkova@sfedu.ru; тел.: 88634393260; кафедра САПР; старший преподаватель.

Yasir Mukhanad Dzhabbar Yasir – Southern Federal University; e-mail: yasir_82@mail.ru; Taganrog, Russia; phone: +78634371625; the department of CAD; postgraduate student.

Gladkov Leonid Anatol'evich – e-mail: lagladkov@sfedu.ru; phone: +78634371625; the department of CAD; cand. of eng. sc.; associate professor.

Gladkova Nadezda Viktorovna — e-mail: nvgladkova@sfedu.ru; phone: +788634393260; the department of CAD; senior teacher.

УДК 004.056 DOI 10.18522/2311-3103-2022-5-17-29

Д.М. Зарубин, В.П. Добрица, Е.А. Титенко

МЕТОД ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ В СИСТЕМЕ ADS-B С ИСПОЛЬЗОВАНИЕМ АППАРАТА КЛЕТОЧНЫХ АВТОМАТОВ

Цель исследования – разработка метода кодирования передаваемых ADS-B сообщений между воздушными судами в процессе полета. Открытый формат 1090ES передаваемых данных является критическим в плане проведения различных типов атак, которые могут привести к нарушению безопасности полетов воздушных судов. Работа направлена на применение средств кодирования и декодирования сообщений с закрытым ключом. Методы исследования основаны на применении и развитии потокового шифрования данных с использованием одномерных клеточных автоматов. Они работают в режиме генератора псевдослучайных последовательностей, преобразующих элементарных состояний ячейки одномерного клеточного автомата на основе типовых аппаратно-ориентированных операций. В основу процессов кодирования и декодирования полей данных положена аналитическое выражение, использующее типовые логические операции (дизъюнкция, сумма по модулю два). Это свойство позволяет вести параллельную обработку полей данных сообщения и создавать неповторяющиеся последовательности кодов. Результаты – создан метод обеспечения защиты передаваемых данных, дополнительно кодирующий на передаче и декодирующий на приеме сообщения. Отличительная особенность метода – сохранение формата протокола. Выполнена оценка вычислительной сложности работы клеточного автомата. Метод использует одномерный клеточный автомат, который выполняет кодирование и декодирование целевых полей (координаты, курс и др.) с использованием генератора псевдослучайных чисел. Разработанный метод относится к классу аппаратно-ориентированных методов. Критические для кодирования и декодирования свойства периодичности полей данных и длины ключа устраняются путем выбора начального иррационального значения и организации «потоковой» работы кодировщика. Если кодирующий автомат работает в потоковом режиме, текущее значение зависит от предыстории некоторой глубины, определение длины «автоматического ключа» из ADS-B сообщения

будет алгоритмически невозможно в силу потери данных. Линейная сложность метода позволяет выполнять преобразования со скоростью потока передачи данных. Вывод – развитие аппаратно-ориентированных методов шифрования данных позволяет повысить эффективность использования системы ADS-B за счет противодействия различным типам деструктивных акций.

Типы атак; псевдослучайная последовательность; функция переходов; кодирование; декодирование.

D.M. Zarubin, V.P. Dobritsa, E.A. Titenko

A METHOD ENCODING TRANSMITTED MESSAGES IN THE ADS-B SYSTEM USING A CELLULAR AUTOMATIC

The purpose of the study is to develop a method for encoding of transmitted ADS-B messages between aircraft. The open format 1090ES of transmitted data is critical in terms of carrying out various types of attacks that can lead to a violation of the safety of aircraft operations. The work is aimed at using means of encoding and decoding messages with a private key. Research methods are based on the application and development of streaming data encryption using one-dimensional cellular automata. They operate as a generator of pseudo-random sequences that transform the elementary states of a cell of a one-dimensional cellular automaton based on typical hardware-oriented operations. The processes of encoding and decoding data fields are based on an analytical expression using typical logical operations (or, xor). This property allows parallel processing of message data fields. The result is the created method for ensuring the protection of transmitted data, additionally encoding on transmission and decoding on message reception. A distinctive feature of the method is the preservation of the protocol forma. The method uses a one-dimensional cellular automaton that encodes and decodes the target fields (coordinates, heading, etc.) using a pseudo-random number generator. The developed method belongs to the class of hardware-oriented methods. Critical for encoding and decoding properties of periodicity of data fields and key length are eliminated by choosing an initial irrational value and organizing the "streaming" work of the encoder. If the encoding automaton is running in streaming mode, the current value depends on the history of some depth, determining the length of the "automatic key" from the ADS-B message will be algorithmically impossible due to data loss. The linear complexity of the method allows you to perform transformations at the data rate. Conclusion: the development of hardware-oriented methods of data encoding makes it possible to increase the efficiency of using the ADS-B system by counteracting various types of destructive actions.

Attack types; pseudo-random sequence; transition function; encoding; decoding.

Введение. Обеспечение безопасности полетов воздушных судов (ВС) в условиях постоянно увеличивающихся пассажиро- и грузопотоков является важной научно-технической задачей. Ее эффективное решение осуществляется в условиях повышения плотности и эшелонирования маршрутов движения ВС, увеличения расстояний маршрутов и их прохождения по экономическим соображениям в удаленных территориях Земли [1].

Радиолокационные системы и наземные радары различных типов являются традиционными стационарными средствами обеспечения мониторинга и, соответственно, организации безопасности воздушного движения. Тем не менее, создаваемая с 70-ых годов XX века сеть стационарных вышек-радаров и стационарных ретрансляторов сигналов от ВС не затрагивает вопросы защиты передаваемых данных в силу исторической не востребованности.

Традиционный подход к отслеживанию движения ВС основан на использовании радиолокационных систем, работающих по принципу идентификации «свой-чужой» (Identification Friend or Foe, IFF), Существенным недостатком данной технологии идентификации является относительно низкая точность, что требует методов и технических средств определения и передачи местоположения ВС, выходящих за рамки возможностей радиолокационных технологий.

Новой технологией мониторинга ВС, которая дополнит традиционные радиолокационные системы, является система автоматического зависимого наблюдения – вещания, Automatic dependent surveillance-broadcast (ADS-B) [2–4]. Самолет, оснащенный средствами широковещательной передачи и приема, позволяет оперативно получать точные данные о характеристиках ВС – сообщения ADS-B (текущие координаты, скорость, курс, абсолютная высота и др.). Тем не менее, эффективность технологии ADS-B ограничена тем, что сообщения ADS-B передаются в открытом формате 1090ES (частота 1090 МГц). Это делает технологию ADS-B уязвимой для внесения изменений в передаваемые данные. Для деструктивных воздействий (атак) на само ВС достаточно недорогого оборудования и специализированного программного обеспечения [5–7].

Можно выделить следующие виды атак, связанные с воздействием на сообщения ADS-B [8–10]:

- несанкционированное подслушивание;
- глушение;
- перехват и рассылка с задержкой;
- модификация.

Таким образом, актуальность работы определяется необходимостью разработки и внедрения метода защиты передаваемых сообщений ADS-B. При этом следует учитывать ограниченные возможности формата сообщений ADS-B, т.е. метод обеспечения защиты создается на основе поиска компромисса между длиной кода и количеством пакетов данных, необходимых для передачи информации.

Постановка задачи. Для исключения внешнего непреднамеренного вмешательства в систему передачи данных ADS-B были предложены подходы к повышению безопасности системы ADS-B, основанные на классификация типов атак с использованием подходов на основе искусственного интеллекта [11,12]. В частности, в последние годы большие распространение получили методы машинного обучения. Эти методы позволяют создавать эффективные алгоритмы прогнозирования и поиска аномалий.

Одним из таких методов является техника фингерпринтинга (техника цифрового отпечатка для сличения с оригиналом), предложенная в работе [13] с целью предотвращения внедрения ложных сообщений в каналы связи ADS-B. Суть фингерпринтинга состоит в сборе данных о фазовой картине электромагнитного излучения при передаче сообщений ADS-B с дальнейшим анализом этой информации с использованием нейронной сети. Данный анализ позволяет с высокой долей вероятности определить является ли сообщение ADS-B модифицированным.

В работе [14, 15] было проведено комплексное исследование, показавшее каким образом классификаторы на основе машинного обучения, могут обнаруживать атаки глушения, нацеленные на каналы передачи данных в системе ADS-B. Несколько алгоритмов машинного обучения, таких как метод опорных векторов, искусственная нейронная сеть и дерево решений, были применены к набору данных с использованием следующих характеристик: частота ошибок по битам, соотношение плохих пакетов и статистическая энергия полученного сигнала. Среди прочего, результаты данного анализа показали перспективность применения нейронных сетей для классификации анализа атак на систему ADS-B.

Однако, несмотря на относительную эффективность подходов, основанных на методах искусственного интеллекта, для выявления и классификации атак одних лишь этих методов недостаточно, так как возможны комбинации атак в различных вариантах.

Известные подходы преимущественно используют потоковые алгоритмы симметричного шифрования, что определяет дополнительные требования к системе ADS-B по скорости трансляции множества сообщений, стойкости шифрующей гамма-последовательности, аппаратной сложности базовых операций прямого и обратного преобразования кодов символов [16–19].

В связи с этим наряду с подходами, основанными на искусственном интеллекте, необходимо разрабатывать и внедрять криптографические решения [20–22], способные обнаруживать или нейтрализовать атаки в системе ADS-B.

Обзор существующих решений. Ранее в научной литературе уже было предложено несколько криптографических подходов для борьбы с некоторыми видами известных атак на систему ADS-B (например, [23–25]). Однако данные исследования показывают, что традиционные криптографические методы нельзя напрямую использовать для защиты ADS-B по ряду причин. С одной стороны, шифрование с использованием традиционных алгоритмов противоречит открытому характеру вещания системы ADS-B. С другой стороны, широковещательный формат трансляции сообщений между ВС приводит к образованию сети множественных (тысячи) трансляций сообщений для их доставки в наземный пункт управления. Вследствие этого внедрение шифрования потоковых данных может привести к большим коммуникационным и вычислительным нагрузкам, что повлияет на эффективность работы всей системы. Применение симметричных алгоритмов шифрования (RSA, MAGMA, AES и др.) [16, 19] влечет дополнительные временные и ресурсные затраты на процессы кодирования и декодирования, что в условиях массовой трансляции ADS-B сообщений достаточно критично в части образования задержек передачи или потерь сообщений. В связи с этим обеспечение конфиденциальности сообщений ADS-B с применением методов и алгоритмов шифрования с линейной вычислительной сложностью является значимой исследовательской задачей.

Метод решения. Канал передачи данных на частоте 1090 МГц, также называемый 1090ES, используется для связи как между самолетами, так и между самолетом и наземными станциями, при этом символ «S» обозначает режим связи «Земля-воздух». Структура передаваемого ADS-B сообщения представлена на рис. 1. Передаваемое сообщение начинается с преамбулы из двух импульсов синхронизации. Затем блок данных передается с использованием позиционно-импульсной модуляции (Pulse Position Modulation, PPM). Поскольку каждый временной интервал имеет длину 1 мкс, бит обозначается отправкой импульса длительностью 0,5 мкс в первой половине интервала (1-бит) или во второй половине (0-бит). В режиме S возможны две разные длины сообщений: 56 бит и 112 бит. Поле формата нисходящей линии связи DF (альтернативно UF для сообщений восходящей линии связи) назначает тип сообщения. Как видно из рис. 1, канал 1090ES использует многоцелевой формат. Установленное значение 17 поля DF указывает, что сообщение имеет расширенный по длине формат, позволяющим передавать 56 произвольных битов в поле ME. Поле CA указывает информацию о возможностях используемого передатчика, а 24-битное поле AA содержит уникальный адрес воздушного судна (ICAO), который позволяет идентифицировать воздушное судно и вести его оперативный мониторинг. Наконец, поле PI предоставляет 24-битный CRC, который позволяет обнаруживать и исправлять возможные ошибки передачи. Более полный обзор ADS-B протокола может быть найден в документах спецификаций [3, 4].

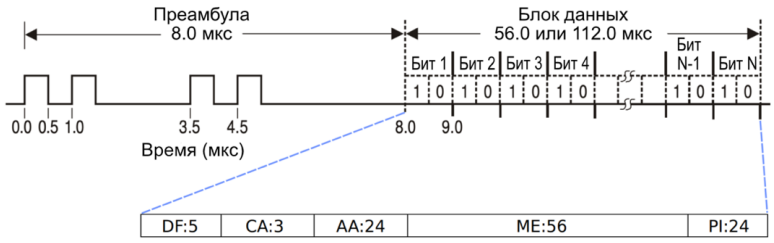

Рис. 1. Структура передаваемого ADS-B сообщения

Анализ структуры ADS-B сообщения, показывает, что 56-битное поле ME может быть использовано для передачи произвольных данных, формируемых перед сеансом связи. Часть этого поля несет позиционные данные и другую информацию. Оставшиеся биты (около 40%) могут быть использованы для реализации решений безопасности, основанных на шифровании передаваемых данных.

В настоящее время распространены два класса алгоритмов шифрования данных:

- системы с секретным ключом;
- системы с открытым ключом.

Одним из перспективных методов криптографии, который можно использовать в сочетании с обоими классами являются клеточные автоматы, предназначенные для генерации псевдослучайных последовательностей. Эти данные являются основой для алгоритмов шифрования.

В общем виде, клеточный автомат представляет собой дискретную динамическую систему, являющуюся совокупностью одинаковых ячеек, соединенных друг с другом одинаковым образом и изменяющих свои состояния во времени. Все клетки образуют так называемую решетку. При этом, решетки могут быть разных видов, отличающихся размерами или формой клетки. Каждая ячейка представляет собой конечный автомат, состояния которого определяются состояниями соседних ячеек и, возможно, ее собственными состояниями.

Простейший одномерный клеточный автомат показан на рис. 2 [26]. Это дискретная структура, представляющая собой совокупность клеток, расположенных в решетке и взаимодействующих по правилу, называемому правилом эволюции. Данное правило определяет переход клеток из текущего состояния в новое состояние за дискретное время t. Для каждой ячейки i, называемой центральной клеткой, определена окрестность радиуса R, состоящая из $n_i = 2R + 1$ ячеек, включая ячейку i. При этом, в зависимости от правила эволюции, преобразования внутри решетки во времени могут быть как линейными, так и нелинейными.

Рис. 3. Пример работы одномерного клеточного автомата за один период дискретного времени

Практическая реализация клеточного автомата должна содержать только конечное число ячеек *N*. Для корректной работы клеточного автомата необходимо задать некоторые граничные условия, определяющие переход крайних ячеек в новое состояние. Известны следующие виды граничных условий:

- фиксированные (ячейки имеют фиксированное значение 0 или 1);
- рефлексивные (зеркальное отражение ячеек по краям решетки);
- циклические (за счет образования круговой сети соединений).

Среди перечисленных типов граничных условий именно циклические обеспечивают наибольшую эффективность генерации псевдослучайных последовательностей и, следовательно, представляют наибольший интерес для создания автоматных шифраторов.

В рамках данной статьи рассматриваются только автоматы, для которых элементарное клеточное состояние $s \in \{0,1\}$. В основе работы клеточного автомата как генератора псевдослучайных чисел (PRNG) [27, 28] используется правило преобразования элементарных состояний ячейки во времени с учетом анализируемой окрестности ячеек *R*:

$$s_i(t+1) = s_{i-1}(t) \oplus (s_i(t) \vee s_{i+1}(t)), \quad (1)$$

где $s_i(t)$ – состояние ячейки i в момент времени t, $s_{i+1}(t)$, $s_{i-1}(t)$ – состояния ячеек i+1, i-1 в момент времени t (окрестность R=1), $s_i(t+1)$ – состояние ячейки i в момент времени t+1.

Псевдослучайные битовые последовательности получаются путем выборки значений, которые целевая ячейка (как правило, это центральная ячейка) достигает по тактам дискретного времени. Исходя из (1) конструкция клеточного автомата имеет довольно простую аппаратную и программную реализацию, так как основана на типовых логических операциях. Данный подход обеспечивает метод шифрования PRNG-данными, формируемыми алгоритмом генерации псевдослучайных чисел с низкой вычислительной сложностью – линейная сложность $\vartheta(N)$. Таким образом, метод шифрования с применением генератора псевдослучайных чисел PRNG имеет большие перспективы для создания систем повышения защищенности каналов связи при сохранении высокой скорости передачи и обработки данных. Схема шифрования канала ADS-B на основе клеточного автомата в режиме генератора псевдослучайных чисел (PRNG) показана на рис. 3.

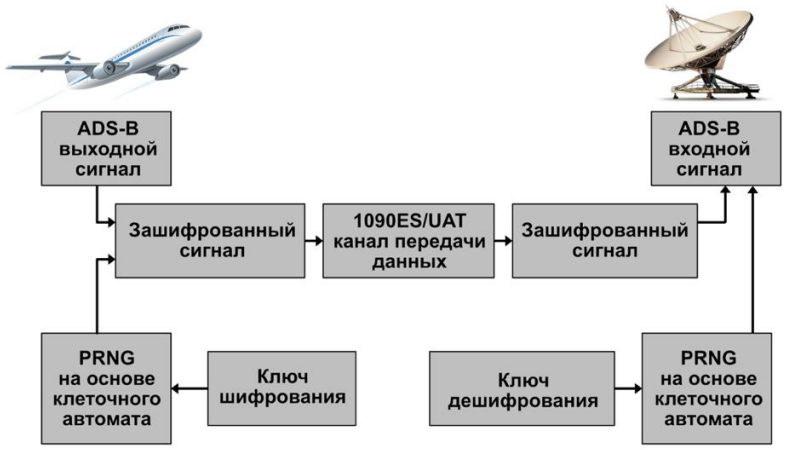

Рис. 3. Схема шифрования канала ADS-B на основе клеточного автомата

В качестве открытого ключа использована комбинация, состоящая из объединения регистрационного номера самолета, адреса Международной организации гражданской авиации (ИКАО), бортового номера или номера рейса, даты и информации о рейсе, что позволяет получить уникальный ключ.

Результаты и обсуждения. Для демонстрации принципа работы шифратора/дешифратора на основе одномерного клеточного автомата будет использоваться реальный сигнал ADS-B.

Структура формата пакета ADS-B показана на рис. 4.

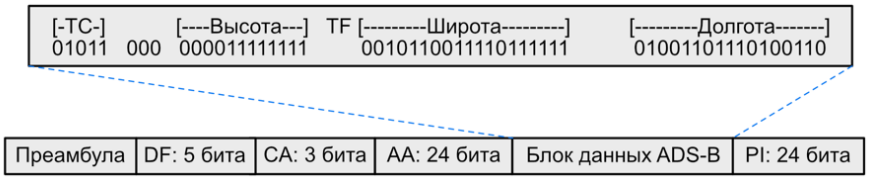

Рис. 4. Сообщение ADS-B с полями блока данных

Как следует из рис. 1 56-ти битный блок данных (ME:56) расположен между 24-ти битным блоком с адресом самолета ИКАО (AA) и 24-ти битным блоком проверки четности (PI). При этом блок данных содержит информацию о высоте, широте и долготе самолета, которая может быть интерпретирована следующим образом: первые 5 бит – это код TC, биты 6 и 7 это статус наблюдения, и бит 8 указывает на используемые антенны. Биты с 9 по 20 содержат информацию о высоте полета воздушного судна. Бит 21 содержит информацию о времени (T). В данном случае этот бит равен 0, что указывает на отсутствие синхронизации с текущем местным временем. Бит 22 указывает на используемый формат отчета о местоположении (четный или нечетный). Биты с 23 по 39 и биты с 40 по 56 содержат закодированную информацию о широте и долготе, соответственно.

Далее рассматривается интерпретация данных о местоположении самолета на примере высоты полета. Блок данных с информацией о высоте полета состоит из 12 бит (биты с 41 по 52). Для интерпретации данного блока информации выполняется следующая процедура:

а) из 12-битного сообщения удаляется 8-й бит, считая от старшего бита, известного как бит Q. Этот бит определяет, сообщается ли высота с приращением 100 футов (Q = 0) или с шагом 25 футов (Q = 1);

б) первые семь битов сдвигаются вправо, что приводит к удалению бита Q. Оставшееся двоичное число затем преобразуется в десятичное, умножается на приращение высоты (25 или 100 футов) и суммируется со значением 1000.

Таким образом, для рассматриваемого в данной статье ADS-B сообщения информация о высоте полета самолёта представлена бинарной комбинацией 000011111111 (рис. 4). Бит Q = 1 указывает на приращение высоты в 25 футов. Удалив 8-й бит, мы получаем двоичное поле - 000001111111, которое эквивалентно числу 127 в десятичной системе. Далее, умножая это число на 25 и прибавляя полученное произведение к 1000, вычисляется результирующая высота – 2175 футов (663 метра).

Процедура кодирования и декодирования информации о местоположении самолета с помощью автоматного шифратора/дешифратора основана на следующих шагах:

- определяется число состояний в клеточном автомате;
- задается функция переходов.

При этом следует учитывать, что любые повторяющиеся числовые последовательности данных в автоматном шифраторе будут снижать криптографическую стойкость, поэтому для построения последовательного автоматный шифратора следует использовать некоторое иррациональное число или генератор псевдослучайных чисел.

Строится структура клеточного автомата из N клеток с помощью исходного иррационального числа на основе правила в виде функции перехода автоматного шифратора (табл. 1). Пусть N-му состояние n в автоматном шифраторе соответствует n-му разряду иррационального числа после запятой.

Таблица 1

Варианты функции перехода автоматного шифратора

n mod 2	Функция перехода	
	Вариант 1	Вариант 2
n mod 2 = 0	0→0 1→1	0→1 1→0
n mod 2 = 1	0→1 1→0	0→0 1→1

Для рандомизации в иррациональном числе также можно брать цифры не подряд, а по некоторому алгоритму. При этом, при определении правила выбора цифр иррационального числа необходимо использовать по одной цифре на состояние, а не на входной символ.

Таким образом, по указанному правилу можно построить автомат длины n. Из-за трансцендентности исходного числа нежелательного свойства периодичности полей данных в «автоматическом ключе» не будет. Также отметим, что поскольку автомат работает в потоковом режиме, определение длины «автоматического ключа» из ADS-B сообщения будет весьма затруднительно, что говорит о криптостойкости метода шифрования.

Далее рассматривается пример работы автоматного шифратора для кодирования сигнала ADS-B на основе поля абсолютной высоты воздушного судна.

Пусть количество состояний клеточного автомата n=6, иррацио-нальное число для шифрования π = 3,1415926535. Для расчета выходных значений автоматного шифратора будет использован вариант 1 из табл. 1. Выходные значения автоматного шифратора показаны в табл. 2.

Таблица 2

Расчет выходных значений автоматного шифратора

Номер состояния	Цифра в π (дробная часть)	Остаток от деления	Выходной символ
0	1	1 mod 2 = 1	0→1 1→0
1	4	4 mod 2 = 0	0→0 1→1
2	1	1 mod 2 = 1	0→1 1→0
3	5	5 mod 2 = 1	0→1 1→0
4	9	9 mod 2 = 1	0→1 1→0
5	2	2 mod 2 = 0	0→0 1→1

На основе построенного автоматного шифратора кодируется информация об высоте полета воздушного судна: 000011111111 (рис. 5).

Как видно из табл. 3, в результате шифрования текста ADS-B сообщения получается преобразование: 000011111111 → 101101010001.

Таблица 3

Шифрование текста ADS-B сообщения автоматным шифратором

Входной символ	0	0	0	0	1	1	1	1	1	1	1	1
Состояние	q_0	q_1	q_2	q_3	q_4	q_5	q_0	q_1	q_2	q_3	q_4	q_5
Выходной символ	1	0	1	1	0	1	0	1	0	0	0	1

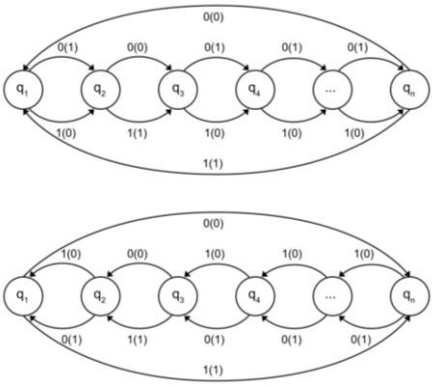

Рис. 5. Схемы кодирования/декодирования данных автоматного шифратора и автоматного дешифратора

Для расшифровки данного сообщения можно воспользоваться автоматным дешифратором, схема смены состояний которого также показана на Рис 5. Можно заметить, что структура автоматного дешифратора аналогична структуре шифратора за исключением изменённых на противоположные направления правил переходов. Начальным состоянием автоматного дешифратора является финальное состояние шифратора.

Таблица 4

Расшифровка текста ADS-B сообщения автоматным дешифратором

Входной символ	1	0	1	1	0	1	0	1	0	0	0	1
Состояние	q_5	q_4	q_3	q_2	q_1	q_0	q_5	q_4	q_3	q_2	q_1	q_0
Выходной символ	0	0	0	0	1	1	1	1	1	1	1	1

Как следует из табл. 4, в результате декодирования получается преобразование 101101010001 → 000011111111, возвращающее исходное ADS-B сообщение.

Выводы

1. Анализ инфраструктуры сети наземных радиолокационных станций-вышек и логическая структура передаваемых ADS-B сообщений не имеют встроенных средств защиты передаваемых данных, что создает уязвимости для канала передачи данных формата 1090ES (расширенный формат).

2. Создан метод обеспечения защиты передаваемых данных на основе одномерного клеточного автомата, выполняющего кодирование и декодирование целевых полей (координаты, курс и др.) с использованием генератора псевдослучайных чисел.

3. Выполнена оценка вычислительной сложности работы клеточного автомата, которая показала перспективность создания систем защиты каналов передачи данных в системе ADS-B на основе применения типовых логических операций кодирования/декодирования целевых полей данных при сохранении исходной скорости передачи данных в системе ADS-B.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Подхалюзина В.А.* Воздушный транспорт в России в условиях глобализации мировой экономики. – LAP LAMBERT Academic Publishing, 2015. – 96 с.
2. *Фальков Э., Шаврин С.* АЗН-В и информационная безопасность воздушного движения // Первая миля. – 2020. – Т. 90, № 5. – С. 50-56.
3. *Рубцов Е.А., Калинцев А.С., Григорьева Е.И.* Анализ линии передачи данных автоматического зависимого наблюдения вещательного типа // Наукоемкие технологии в космических исследованиях Земли. – 2018. – Т. 10, № 6. –С. 19-27.
4. *Николаев К.А.* Описание систем автоматического зависимого наблюдения-вещания и их преимущества перед радиолокацией // Естественные и технические науки. – 2018. – № 4. – С. 38-40.
5. *Большаков А.А.* Метод распознавания угрозы авиационного происшествия на базе искусственного интеллекта // Математические методы в технике и технологиях. – 2017. – Т. 4. – С. 90-95.
6. *Ying X. et al.* Detecting ADS-B Spoofing Attacks using Deep Neural Networks // 2019 IEEE Conference on Communications and Network Security, CNS 2019. Institute of Electrical and Electronics Engineers Inc. – 2019. – P. 187-195.
7. *Schäfer M., Lenders V., Martinovic I.* Experimental Analysis of Attacks on Next Generation Air Traffic Communication // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). – Springer, Berlin, Heidelberg, 2013. – Vol. 7954 LNCS. – P. 253-271.
8. *McCallie D., Butts J., Mills R.* Security analysis of the ADS-B implementation in the next generation air transportation system // International Journal of Critical Infrastructure Protection. – 2011. – Vol. 4, No. 2. – P. 78-87.
9. *Grover K., Lim A., Yang Q.* Jamming and anti-jamming techniques in wireless networks: A survey // International Journal of Ad Hoc and Ubiquitous Computing. – 2014. – Vol. 17, No. 4. – P. 197-215.
10. *Riahi Manesh M., Kaabouch N.* Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system // International Journal of Critical Infrastructure Protection. – 2017. – Vol. 19. – P. 16-31.
11. *Большаков А.А., Кулик А.А.* Повышение безопасности полета воздушного судна с использованием методов искусственного интеллекта // Математические методы в технике и технологиях. – 2019. – Т. 11. – С. 87-99.
12. *Schäfer M., Lenders V., Martinovic I.* Experimental Analysis of Attacks on Next Generation Air Traffic Communication // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). – Springer, Berlin, Heidelberg, 2013. – Vol. 7954 LNCS. – P. 253-271.
13. *Leonardi M., di Gregorio L., di Fausto D.* Air Traffic Security: Aircraft Classification Using ADS-B Message's Phase-Pattern // Aerospace. – 2017. – Vol. 4. – P. 51.
14. *Manesh M.R. et al.* Performance Comparison of Machine Learning Algorithms in Detecting Jamming Attacks on ADS-B Devices // 2019 IEEE International Conference on Electro Information Technology (EIT). – IEEE, 2019. – P. 200-206.
15. *Kacem T. et al.* ADS-B Attack Classification using Machine Learning Techniques // 2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops). – IEEE, 2021. – P. 7-12.
16. *Кондаков С.Е., Рудь И.С.* Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. – 2021. – № 5(45). – С. 12-20.
17. *Фомичев В.М.* Методы дискретной математики в криптологии. – М.: МИФИ, 2010. – 424 с.
18. *Шнайер Б.* Прикладная криптография. – М.: Триумф, 2002. – 816 с.

19. *Ставер Е.В.* Алгоритм RSA. Шифрование и дешифрование текстовых сообщений // Научный аспект. – 2012. – № 3. – С. 88-89.
20. *Finke C., Butts J., Mills R.* ADS-B encryption // Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13. – New York, New York, USA: ACM Press, 2013. – P. 1.
21. *Zhang J., Wei L., Yanbo Z.* Study of ADS-B Data Evaluation // Chinese Journal of Aeronautics. – 2011. – Vol. 24. – P. 461-466.
22. *Yang H. et al.* A practical and compatible cryptographic solution to ADS-B security // IEEE Internet of Things Journal. Institute of Electrical and Electronics Engineers Inc. – 2019. – Vol. 6, No. 2. – P. 3322-3334.
23. *Strohmeier M. et al.* On the security of the automatic dependent surveillance-broadcast protocol // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, No. 2. – P. 1066-1087.
24. *Sampigethaya K. et al.* Future e-enabled aircraft communications and security: The next 20 years and beyond // Proceedings of the IEEE. – 2011. – Vol. 99, No. 11. – P. 2040-2055.
25. *H. Ren H. et al.* Querying in Internet of Things with privacy preserving: Challenges solutions and opportunities // IEEE Network. – 2018. – Vol. 32, No. 6. – P. 144-151.
26. *Соколов А.В.* Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов // Праці Одеського політехнічного університету. – 2014. – Vol. 1, No. 43. – P. 180-186.
27. *Wolfram S.* Random sequence generation by cellular automata // Advances in Applied Mathematics. – 1986. – Vol. 7, No. 2. – P. 123-169.
28. *Cook E.* ADS-B, Friend or Foe: ADS-B Message Authentication for NextGen Aircraft // 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems. – IEEE, 2015. – P. 1256-1261.

REFERENCES

1. *Podkhalyuzina V.A.* Vozdushnyy transport v Rossii v usloviyakh globalizatsii mirovoy ekonomiki [Air transport in Russia in the context of the globalization of the world economy]. LAP LAMBERT Academic Publishing, 2015, 96 p.
2. *Fal'kov E., Shavrin S.* AZN-V i informatsionnaya bezopasnost' vozdushnogo dvizheniya [AZN-V and information security of air traffic], *Pervaya milya* [The first mile], 2020, Vol. 90, No. 5, pp. 50-56.
3. *Rubtsov E.A., Kalintsev A.S., Grigor'eva E.I.* Analiz linii peredachi dannykh avtomaticheskogo zavisimogo nablyudeniya veshchatel'nogo tipa [Analysis of the data transmission line of automatic dependent observation of broadcast type], *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [High–tech technologies in space research of the Earth], 2018, Vol. 10, No. 6, pp. 19-27.
4. *Nikolaev K.A.* Opisanie sistem avtomaticheskogo zavisimogo nablyudeniya-veshchaniya i ikh preimushchestva pered radiolokatsiey [Description of automatic dependent surveillance-broadcasting systems and their advantages over radar], *Estestvennye i tekhnicheskie nauki* [Natural and technical sciences], 2018, No. 4, pp. 38-40.
5. *Bol'shakov A.A.* Metod raspoznavaniya ugrozy aviatsionnogo proisshestviya na baze iskusstvennogo intellekta [The method of recognizing the threat of an aviation accident based on artificial intelligence], *Matematicheskie metody v tekhnike i tekhnologiyakh* [Mathematical methods in engineering and technology], 2017, Vol. 4, pp. 90-95.
6. *Ying X. et al.* Detecting ADS-B Spoofing Attacks using Deep Neural Networks, *2019 IEEE Conference on Communications and Network Security, CNS 2019. Institute of Electrical and Electronics Engineers Inc*., 2019, pp. 187-195.
7. *Schäfer M., Lenders V., Martinovic I.* Experimental Analysis of Attacks on Next Generation Air Traffic Communication, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer, Berlin, Heidelberg, 2013, Vol. 7954 LNCS, pp. 253-271.
8. *McCallie D., Butts J., Mills R.* Security analysis of the ADS-B implementation in the next generation air transportation system,/ *International Journal of Critical Infrastructure Protection*, 2011, Vol. 4, No. 2, pp. 78-87.

9. *Grover K., Lim A., Yang Q.* Jamming and anti-jamming techniques in wireless networks: A survey, *International Journal of Ad Hoc and Ubiquitous Computing*, 2014, Vol. 17, No. 4, pp. 197-215.
10. *Riahi Manesh M., Kaabouch N.* Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system, *International Journal of Critical Infrastructure Protection*, 2017, Vol. 19, pp. 16-31.
11. *Bol'shakov A.A., Kulik A.A.* Povyshenie bezopasnosti poleta vozdushnogo sudna s ispol'zovaniem metodov iskusstvennogo intellekta [Improving the safety of aircraft flight using artificial intelligence methods], *Matematicheskie metody v tekhnike i tekhnologiyakh* [Mathematical methods in engineering and technology], 2019, Vol. 11, pp. 87-99.
12. *Schäfer M., Lenders V., Martinovic I.* Experimental Analysis of Attacks on Next Generation Air Traffic Communication, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer, Berlin, Heidelberg, 2013, Vol. 7954 LNCS, pp. 253-271.
13. *Leonardi M., di Gregorio L., di Fausto D.* Air Traffic Security: Aircraft Classification Using ADS-B Message's Phase-Pattern, *Aerospace*, 2017, Vol. 4, pp. 51.
14. *Manesh M.R. et al.* Performance Comparison of Machine Learning Algorithms in Detecting Jamming Attacks on ADS-B Devices, *2019 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2019, pp. 200-206.
15. *Kacem T. et al.* ADS-B Attack Classification using Machine Learning Techniques, *2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops*). IEEE, 2021, pp. 7-12.
16. *Kondakov S.E., Rud' I.S.* Model' protsessa provedeniya komp'yuternykh atak s ispol'zovaniem spetsial'nykh informatsionnykh vozdeystviy [A model of the process of conducting computer attacks using special information influences], *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2021, No. 5 (45), pp. 12-20.
17. *Fomichev V.M.* Metody diskretnoy matematiki v kriptologii [Methods of discrete mathematics in cryptology]. Moscow: MIFI, 2010, 424 p.
18. *Shnayer B.* Prikladnaya kriptografiya [Applied cryptography]. Moscow: Triumf, 2002, 816 p.
19. *Staver E.V.* Algoritm RSA. Shifrovanie i deshifrovanie tekstovykh soobshcheniy [The RSA algorithm. Encryption and decryption of text messages], *Nauchnyy aspect* [Scientific aspect], 2012, No. 3, pp. 88-89.
20. *Finke C., Butts J., Mills R.* ADS-B encryption, *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13*. New York, New York, USA: ACM Press, 2013, pp. 1.
21. *Zhang J., Wei L., Yanbo Z.* Study of ADS-B Data Evaluation, *Chinese Journal of Aeronautics*, 2011, Vol. 24, pp. 461-466.
22. *Yang H. et al.* A practical and compatible cryptographic solution to ADS-B security, *IEEE Internet of Things Journal. Institute of Electrical and Electronics Engineers Inc.*, 2019, Vol. 6, No. 2, pp. 3322-3334.
23. *Strohmeier M. et al.* On the security of the automatic dependent surveillance-broadcast protocol, *IEEE Communications Surveys & Tutorials*, 2015, Vol. 17, No. 2, pp. 1066-1087.
24. *Sampigethaya K. et al.* Future e-enabled aircraft communications and security: The next 20 years and beyond, *Proceedings of the IEEE*, 2011, Vol. 99, No. 11, pp. 2040-2055.
25. *H. Ren H. et al.* Querying in Internet of Things with privacy preserving: Challenges solutions and opportunities, *IEEE Network*, 2018, Vol. 32, No. 6, pp. 144-151.
26. *Sokolov A.V.* Bystrodeystvuyushchiy generator klyuchevykh posledovatel'nostey na osnove kletochnykh avtomatov [A high-speed generator of key sequences based on cellular automata], *Pratsi Odes'kogo politekhnichnogo universitetu* [Proceedings of Odessa Polytechnic University], 2014, Vol. 1, No. 43, pp. 180-186.
27. *Wolfram S.* Random sequence generation by cellular automata, *Advances in Applied Mathematics*, 1986, Vol. 7, No. 2, pp. 123-169.
28. *Cook E.* ADS-B, Friend or Foe: ADS-B Message Authentication for NextGen Aircraft, *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*. IEEE, 2015, pp. 1256-1261.

Статью рекомендовал к опубликованию д.т.н., профессор А.Н. Целых.

Зарубин Денис Михайлович – Юго-Западный государственный университет; e-mail: orion-589@yandex.ru; г. Курск, Россия; научный сотрудник научно-исследовательского института космического приборостроения и радиоэлектронных систем.

Добрица Вячеслав Порфирьевич – e-mail: dobritsa@mail.ru; профессор кафедры защиты информации; д.ф.-м.н.

Титенко Евгений Анатольевич – e-mail: johntit@mail.ru; тел.: +79051588904; ведущий научный сотрудник научно-исследовательского института космического приборостроения и радиоэлектронных систем; к.т.н.

Zarubin Denis Mikhailovich – South-West State University; e-mail: orion-589@yandex.ru; Kursk, Russia; researcher at the Research Institute of Space Instrumentation and Radioelectronic Systems.

Dobritsa Vyacheslav Porfiryevich – e-mail: dobritsa@mail.ru; professor of the Information Security Department; dr. of phys. and math. sc.

Titenko Evgeny Anatolyevich – e-mail: johntit@mail.ru; phone: +79051588904; leading researcher of the Research Institute of Space Instrumentation and Radioelectronic Systems; cand. of eng. sc.

УДК 517.524 DOI 10.18522/2311-3103-2022-5-29-37

В.Е. Долгой, И.Э. Гамолина

АЛГОРИТМ РЕШЕНИЯ ПРИВЕДЕННОГО ПОЛИНОМИАЛЬНОГО УРАВНЕНИЯ С ПОМОЩЬЮ НЕПРЕРЫВНЫХ ДРОБЕЙ

Приводится алгоритм, основанный на применении непрерывных дробей, для нахождения нулей полинома n-й степени. В настоящее время существует большое разнообразие методов и алгоритмов для решения задач подобного типа; отличительной особенностью предлагаемого алгоритма является возможность его эффективного использования при достаточно больших значениях n, кроме того, данный алгоритм применим в случае наличия комплексных корней. Любое действительное число можно представить в виде конечной или бесконечной непрерывной цепной дроби. Основное назначение цепных дробей состоит в том, что они дают малую погрешность при приближенных вычислениях действительных чисел в виде обыкновенных дробей при решении алгебраических уравнений и систем. Целью нашей работы является применение разработанного алгоритма для решения полиномиальных уравнений, содержащих не только действительные, но и комплексные корни, с помощью непрерывных дробей; оценка числа арифметических шагов при его численном решении. В статье приводятся аналитические выражения для решения полиномиального уравнения; полученные аналитические выражения представляют собой отношение определителей Теплица. Отличительной особенностью данных определителей является наличие в качестве диагональных элементов коэффициентов решаемого алгебраического уравнения. Для получения численного решения использован модифицированный алгоритм Рутисхаузера. Комплексные корни при решении уравнения могут быть найдены с помощью алгоритма для суммирования непрерывных дробей. В статье приводятся в качестве иллюстрации предлагаемого алгоритма результаты численного решения полиномиального уравнения пятой степени. Преимуществом алгоритма является малое количество затрачиваемых арифметических операций, возможность рассмотрения полиномов высокой степени, малая погрешность вычислений.

Модифицированный алгоритм Рутисхаузера; непрерывные дроби; алгоритм суммирования расходящихся непрерывных дробей; определители Теплица; r/φ-алгоритм.