ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

DOI 10.21672/2074-1707.2021.53.1.062-070
УДК 004.421.5

ВАРИАНТ АЛГОРИТМА ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ОСНОВАННЫЙ НА СВОЙСТВАХ ЛИНЕЙНЫХ КЛЕТОЧНЫХ АВТОМАТОВ[1]

Статья поступила в редакцию 30.03.2021, в окончательном варианте – 30.04.2021.

Кулешова Елена Александровна, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
аспирант, ORCID 0000−0002−8270−564X, e-mail: lena.kuleshova.94@mail.ru
Марухленко Анатолий Леонидович, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
кандидат технических наук, доцент, ORCID 0000−0002−3575−924X, e-mail: proxy33@mail.ru
Добрица Вячеслав Порфирьевич, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
доктор физико-математических наук, профессор, ORCID 0000−0001−7533−3684, e-mail: dobritsa@mail.ru
Таныгин Максим Олегович, Юго-Западный государственный университет, 305004, Российская Федерация я, г. Курск, ул. Челюскинцев, 19, корпус Б,
кандидат технических наук, доцент, ORCID 0000−0002−4099−1414, e-mail: tanygin@yandex.ru
Плугатарев Алексей Владимирович, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19, корпус Б,
аспирант, ORCID 0000-0002-8549-4382, e-mail: aplugatarev@bk.ru

Статья посвящена разработке линейной системы генерации псевдослучайной последовательности на основе клеточных автоматов, разработка модели для нескольких генераторов нелинейных псевдослучайных последовательностей с практическими приложениями в системах симметричного преобразования данных. Такая модель генерирует все решения линейных бинарных разностных уравнений. Важно отметить, что многие из этих решений представляют собой псевдослучайные последовательности ключевого потока. В процессе разработки линейной системы на основе клеточных автоматов рассматриваются две основные структуры: линейные разностные уравнения и одномерные линейные гибридные клеточные автоматы. В данной статье показано, что все решения линейных бинарных разностных уравнений могут быть реализованы с помощью линейных моделей на основе клеточных автоматов с применением «правила 90» и «правила 150». Разработана модель генерации псевдослучайных битовых последовательностей, наиболее применимая в системах связи с высокой скоростью передачи. Основным отличием данной модели является то, что она построена на исключительно последовательной конкатенации базового линейного автомата, что обуславливает простоту предлагаемой модели. Также был предложен алгоритм контроля целостности и аутентичности блочных данных на основе предложенного алгоритма генерации псевдослучайной последовательности. Практическая значимость состоит в том, что предложенная модель проста и может применяться в системах защиты информации на практике, в том числе в системах контроля аутентификации и целостности данных.

Ключевые слова: информационная безопасность, потоковая передача данных, клеточные автоматы, псевдослучайные двоичные последовательности, системы защиты конфиденциальной информации

A VARIANT OF THE ALGORITHM FOR GENERATING PSEUDO-RANDOM BINARY SEQUENCES BASED ON THE PROPERTIES OF LINEAR CELLULAR AUTOMATA

The article was received by the editorial board on 30.03.2021, in the final version – 30.04.2021.

Kuleshova Elena A., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
graduate student, ORCID 0000−0002−8270−564X, e-mail: lena.kuleshova.94@mail.ru

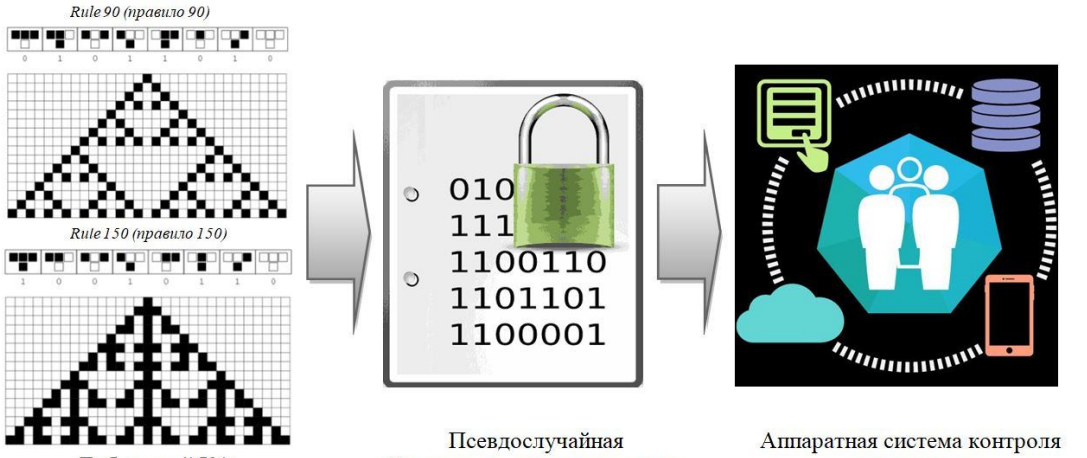
[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-31-90069

Marukhlenko Anatoly L., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID 0000-0002-3575-924X, e-mail: proxy33@mail.ru
Dobritsa Vyacheslav P., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
Doct. Sci. (Physical and Mathematical), Professor, ORCID 0000-0001-7533-3684, e-mail: dobritsa@mail.ru
Tanygin Maxim O., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID 0000-0002-4099-1414, e-mail: tanygin@yandex.ru
Plugatarev Alexey V., Southwest State University, building B, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,
graduate student, ORCID 0000-0002-8549-4382, e-mail: aplugatarev@bk.ru

The article is devoted to the development of a linear system for generating a pseudo-random sequence based on cellular automata, the development of a model for several generators of nonlinear pseudo-random sequences with practical applications in symmetric data transformation systems. Such a model generates all solutions to linear binary difference equations. It is important to note that many of these solutions are pseudo-random keystream sequences. In the process of developing a linear system based on cellular automata, two main structures are considered: linear difference equations and one-dimensional linear hybrid cellular automata. This article shows that all solutions to linear binary difference equations can be implemented using linear models based on cellular automata using the "rule 90" and "rule 150". A model for generating pseudo-random bit sequences has been developed, which is most applicable in communication systems with a high transmission rate. The main difference of this model is that it is built on an exclusively sequential concatenation of a basic linear automaton, which determines the simplicity of the proposed model. Also, an algorithm for controlling the integrity and authenticity of block data was proposed based on the proposed algorithm for generating a pseudo-random sequence. The practical significance lies in the fact that the proposed model is simple and can be applied in information security systems in practice, including in authentication and data integrity control systems.

Keywords: information security, data streaming, cellular automata, pseudo-random binary sequences, confidential information protection systems

Graphical annotation (Графическая аннотация)



Гибридный КА (Hybrid CA) | Псевдослучайная бинарная последовательность (Pseudo-Random Binary Sequence) | Аппаратная система контроля целостности (Hardware Integrity Control System)

Введение. Применение клеточных автоматов для генерации псевдослучайных последовательностей началось С. Вольфрамом, когда был предложен способ сокрытия данных, использующий генератор псевдослучайных последовательностей на основе одномерного клеточного автомата с периодическими границами и с использованием правила 30.

Клеточный автомат (КА) состоит из набора ячеек, организованных в виде регулярной сети. Каждая ячейка КА – это конечный автомат, который использует множество конечных состояний. Выделяют следующие основные свойства КА – дискретность, локальное взаимодействие, однородность и параллельную эволюцию [1]. Каждый год авторы посвящают клеточным автоматам большое

количество научных работ. Главная причина популярности КА, несмотря на их простоту, состоит в огромном потенциале, которым они обладают в моделировании сложных систем [2].

Главная цель данной статьи – это создание алгоритма генерации псевдослучайных бинарных последовательностей, основываясь на свойствах линейных клеточных автоматов. Данные последовательности используются в качестве ключа в поточных шифрах. Поточный шифр – это шифр симметричного способа шифрования, в котором каждый символ исходного текста преобразуется в символ шифротекста, в зависимости от используемого ключа.

В отличие от методов блочного преобразования данных при поточной обработке производится преобразование одного бита за одну операцию [3]. При применении поточного алгоритма шифрования отсутствует необходимость разбивать сообщение на целое число блоков достаточно большой длины. Таким образом, поточный шифр может работать в реальном времени, то есть, если передается поток символов, каждый символ может шифроваться и передаваться сразу [4, 5]. Также в данной статье был предложен алгоритм контроля целостности и аутентичности и блочных данных на основе предложенного алгоритма генерации псевдослучайной последовательности.

На данный момент в различных исследованиях представлено довольно большое разнообразие семейств псевдослучайных последовательностей [6]. Среди них стоит выделить псевдослучайные последовательности, основанные на регистрах сдвига с линейной обратной связью. Выходные последовательности таких типов определяются с помощью нелинейных функций для создания последовательностей бинарного потока ключей. Они могут генерироваться разными способами [7].

В данной работе показано, что одномерные линейные КА на основе правил 90/150 генерируют все решения линейных разностных уравнений с двоичными постоянными коэффициентами. Некоторые из этих решений соответствуют сгенерированным псевдослучайным потокам ключей. Таким образом, разработан простой КА, который является линейной моделью генерации нелинейной псевдослучайной битовой последовательности. Из-за линейности правил перехода КА моделирование этих основанных на КА структур является простым и эффективным.

Постановка задачи. Генерация псевдослучайных чисел – одна из важнейших задач в области защиты данных. Генераторы случайных чисел используются не только для генерации ключей, но и в других важных частях алгоритмов и протоколов защиты информации. Генератор псевдослучайных чисел – это детерминированный алгоритм, который производит числа, распределение которых неотличимо от равномерного.

В классическом случае сгенерированный случайный поток используется в качестве ключевого потока, с которым можно выполнить операцию XOR для открытого текста. Случайное число получается из центральной ячейки решетки КА. Затем в результате непрерывной эволюции КА получается поток случайных чисел. Выбор центральной ячейки в качестве источника случайных битов был основан на том, что в этой ячейке не было значимых статистических закономерностей.

В настоящее время регистры сдвига с линейной обратной связью являются наиболее популярной техникой при разработке генераторов псевдослучайных потоков из-за их компактной и простой конструкции. В контексте данной работы рассматривается задача генерации псевдослучайных бинарных последовательностей всех решений линейных разностных уравнений с учетом оператора сдвига.

Материалы и методы. Данный раздел посвящен краткому рассмотрению двух основных структур, использованных при разработке модели генератора бинарных последовательностей (линейные разностные уравнения и одномерные гибридные КА).

Линейные разностные уравнения. Рассмотрим следующие линейные разностные уравнения, учитывая бинарные коэффициенты:

$$(E^r \oplus \sum_{j=1}^{r} c_j E^{r-j}) a_n = 0,\ n \geq 0, \tag{1}$$

где $a_n \in GF(2)$ – n-й член двоичной последовательности $\{a_n\}$. $E_j = a_n + j$ – оператор сдвига, определяемый с учетом хронологии решений. $c_j \in GF(2)$ – постоянный двоичный коэффициент, r – целое число, а символ $\oplus$ в данном контексте определяет операцию *XOR*. Характеристический многочлен r-степени уравнения (1) равен:

$$P(x) = x^r + \sum_{j=1}^{r} c_j x^{r-j} \tag{2}$$

и определяет отношение линейного повторения последовательности $\{a_n\}$. Это означает, что его n-й член a_n может быть записан как линейная комбинация предыдущих членов:

$$(a_n \oplus \sum_{j=1}^{r} c_j a_{n-j}) a_n = 0,\ n \geq r\,. \tag{3}$$

В дальнейшем $P(x)$ будет рассматривать в качестве тривиального полинома двоичных коэффициентов. При этом, если a – один из корней рассматриваемого полинома, то

$$a, a^2, a^{2^2}, ..., a^{2^{(r-1)}} \in GF(2^r), \tag{4}$$

где r – множество корней многочлена. В этом случае решения уравнения (1) представляют собой последовательности вида:

$$a_n = \sum_{j=0}^{r-1} A^{2^j} a^{2^j n}, n \geq 0, \tag{5}$$

где A – произвольный элемент из $GF(2^r)$. Другими словами, $\{a_n\}$ – это последовательность псевдо шума (PN-последовательность) характеристического полинома $P(x)$ и периода $2^{(r-1)}$, чья начальная точка определяется значением A. Если $A=0$, то решение уравнения (1) – это тождественно нулевая последовательность.

Одномерный линейный гибридный клеточный автомат. Для выделения свойств линейных клеточных автоматов перейдем к рассмотрению гибридного линейного КА. Определим правила перехода, которые позволят привести КА к нетривиальным структурам [8].

Правила определяется кодом Вольфрама как «правило 90» и «правило 150». Оба правила определяются следующим образом:

1. Правило 90: $b_{n+1}^k = b_n^{k-1} \oplus b_n^{k+1}$.

2. Правило 150: $b_{n+1}^k = b_n^{k-1} \oplus b_n^k \oplus b_n^{k+1}$.

Таким образом, в момент времени $n+1$ содержимое k-й ячейки $b_{n+1}^k \in GF(2)$ зависит от содержимого в момент времени n либо двух разных ячеек (правило 90), либо трех разных ячеек (правило 150), где $k = 1,...,L$, где L – длина автомата. При этом двоичное содержимое L ячеек определяется состоянием автомата в момент времени n. Формальная форма записи автоматов данного типа дается L-набором $\Delta L = (d_1, d_2, ..., d_L)$, где $d_k = 0$, если k-я ячейка проверяет правило 90, в то время как $d_k = 1$, если k-я ячейка проверяет правило 150. Кроме того, $\Delta k = (d_1, d_2, ..., d_k)$, где $k = 1,...,L$ обозначает соответствующий подавтомат длины k.

На основе алгоритма синтеза Кеттелла и Муцио [9] получим два линейных 90/150 КА с характеристическим полиномом $Q(x)$. Следовательно, одномерный двоичный линейный клеточный автомат 90/150 с примитивным характеристическим полиномом $P(x)$, заданным формулой (2) будет генерировать PN-последовательность, определенную уравнением (5), данная последовательность в таблице 1 выделена жирным шрифтом. Далее перейдем к рассмотрению следующих вопросов:

1. Как решение уравнения (1) с характеристическим полиномом $P(x) = x^3 + x^2 + 1,\ r = 3$ и $A = 1$ $(a \in GF(2_3))$:

$$a_n = 1a^n \oplus 1a^{2n} \oplus 1a^{4n},\ n \geq 0\,. \tag{6}$$

2. Как последовательность, генерируемая парой обратных КА, начиная с начальных состояний (1,0,1) и (1,1,0) соответственно. В остальных ячейках КА сдвинутые версии той же сгенерированной PN-последовательности.

Таблица 1 – PN-последовательность, полученная либо как решение разностного уравнения, либо как последовательность, порожденная двумя обратными линейными КА

	Начальное состояние						
	1	**1**	**1**	**0**	**1**	**0**	**0**
	КА						
150	**1**	**1**	**1**	**0**	**1**	**0**	**0**
90	0	0	1	1	1	0	1
90	1	0	0	1	1	1	0
150	**1**	**1**	**1**	**0**	**1**	**0**	**0**
90	1	1	0	1	0	0	1
90	0	1	0	0	1	1	1

Обобщение. Обобщим разностные уравнения в более сложную разновидность линейных разностных уравнений, корни которых имеют кратность больше 1. Фактически мы собираемся рассматривать уравнения вида:

$$(E^r \oplus \sum_{j=1}^{r} c_j E^{r-j})^p a_n = 0,\ n \geq 0, \tag{7}$$

где p – целое число > 1. Таким образом, характеристический многочлен $P_M(x)$ будет иметь вид:

$$P_M(x) = P(x)^p = (x^r + \sum_{j=1}^{r} c_j x^{r-j})^p . \tag{8}$$

Получаем корни многочлена $P_M(x)$ и видим, что они совпадают с корнями у многочлена $P(x)$, т.е. $a, a^2, a^{2^2}, ..., a^{2^{(r-1)}}$, но с кратностью p. Таким образом, решение уравнения (7) будет иметь следующий вид:

$$a_n = \sum_{i=i}^{p-1} \left(\binom{n}{i} \sum_{j=0}^{r-1} A_i^{2^j} a^{2^j n} \right), \tag{9}$$

где A_i – произвольный элемент из $GF(2^r)$; $\binom{n}{i}$ – количество всех подмножеств размера i в n-м элементе (биноминальный коэффициент). В соответствии с уравнением (5) для последовательности с начальной точкой в A_i n-й элемент определяется как $\sum_{j=0}^{r-1} A_i^{2^j} a^{2^j n}$, из чего следует, что двоичная последовательность будет являться побитовой суммой одной и той же PN-последовательности, берущей начало из разных точек, при этом последовательность двоичных значений будет определяться коэффициентами $\binom{n}{i}$, период T_i остается постоянным. В таблице 2 представлены бинарные значения и значения периодов для коэффициентов $i = 0,...,7$.

Характеристики бинарной последовательности определяются биноминальными коэффициентами A_i, являющимися решениями (7). Количество различных бинарных последовательностей определяется количеством различных p-кортежей значений A_i. Уравнения вида (7) в данном контексте имеют особое значение, это связано с тем, что упомянутые во введении двоичные последовательности имеют характеристические многочлены вида (8). Следовательно, многие двоичные последовательности – это решения уравнений вида (7).

Таблица 2 – Бинарные значения и периоды для биномиальных коэффициентов

Бинарные значения	**Периоды** T_i	**Биноминальные коэффициенты** $\binom{n}{i}$
1,1,1,1,1,1,1,1,1,1, …	$T_1 = 1$	$i = 0$
0,1,0,1,0,1,0,1,0,1, …	$T_2 = 2$	$i = 1$
0,0,1,1,0,0,1,1,0,0, …	$T_3 = 4$	$i = 2$
0,0,0,1,0,0,0,1,0,0, …	$T_4 = 4$	$i = 3$
0,0,0,0,1,1,1,1,0,0, …	$T_5 = 8$	$i = 4$
0,0,0,0,0,1,0,1,0,0, …	$T_6 = 8$	$i = 5$
0,0,0,0,0,0,1,1,0,0, …	$T_7 = 8$	$i = 6$
0,0,0,0,0,0,0,1,0,0, …	$T_8 = 8$	$i = 7$

Из вышесказанного можно сделать вывод о необходимости разработки простой линейной модели, позволяющей находить все решения этих разностных уравнений, с целью нахождения среди них псевдослучайных последовательностей.

Результаты и их обсуждение. Решение линейных разностных уравнений с помощью КА. В данной работе предлагается решение линейных разностных уравнений с помощью КА на основе конкатенации p раз базового автомата (так как $P_M(x) = P(x)^p$), при этом для каждого $P(x)$ существуют два обратных базовых автомата, которые могут использоваться в процедуре конкатенации.

Результат можно повторять несколько раз для последовательных многочленов и векторы правил:

$$P(x) \leftrightarrow \Delta_L = (d_1, d_2, \ldots, d_L)$$
$$P(x)^2 \leftrightarrow \Delta_{2L} = (d_1, d_2, \ldots, d_L, d_L, \ldots, d_2, d_1)$$
$$P(x)^{2^2} \leftrightarrow \Delta_{2^2 L} = (d_1, d_2, \ldots, d_L, d_L, \ldots, d_2, d_1, d_1, d_2, \ldots, d_L, d_L, \ldots, d_2, d_1)$$
$$\vdots \leftrightarrow \vdots \quad \vdots$$

Таким образом, получаем КА, характеристические многочлены которого: $P(x)^2, P(x)^{2^2}, P(x)^{2^3}, \ldots, P(x)^{2^q}$ длины $2L, 2^2 L, 2^3 L, \ldots, 2^q L$ соответственно.

Численное моделирование. В качестве примера рассмотрим пару обратных КА, длиной L = 5, связанных с характеристическим многочленом $P(x) = x^5 + x^4 + x^2 + x + 1$ (первый автомат (1,0,0,0,0), второй автомат (0,0,0,0,1)). Если $P_M(x) = P(x)^p$ при p = 4, то один из КА, полученных путем конкатенации, будет иметь вид (1,0,0,0,1,1,0,0,0,0,0,0,0,0,1,1,0,0,0,1), а его длина составит L =10. Различные варианты A_i (не все нулевые) позволят нам сгенерировать решения уравнения (7).

1. Если $A_0 \neq 0$ и $A_i = 0, \ \forall_i > 0$, то клеточный автомат выдаст уникальную PN-последовательность $N_0 = 1$ последовательность периода $T_0 = 31$, линейная сложность которой составит $LC_0 = 5$ и характеристический многочлен $P(x)$. Кроме того, автоматные циклы дважды симметричны: $a_0, a_1, a_2, a_3, a_4, a_4, a_3, a_2, a_1, a_0, a_0, a_1, a_2, a_3, a_4, a_4, a_3, a_2, a_1, a_0$ с $a_j \in GF(2)$. 31-е дважды симметричное состояние сосредоточено в одном и том же цикле.

2. Если $A_1 \neq 0$ и $A_i = 0, \ \forall_i > 1$, то клеточный автомат выдаст $N_1 = 16$ различных последовательностей периода $T_1 = 62$, линейная сложность $LC_1 = 10$ и характеристический многочлен $P(x)^2$. Кроме того, автомат проходит через симметричные состояния следующего вида: $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_9, a_8, a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0$ с $a_j \in GF(2)$. Существует 210–32 = 992 симметричных состояний, распределенных в 16 циклах по 62 состояния в каждом из них.

3. Если $A_2 \neq 0$ и $A_i = 0, \ \forall_i > 2$, то клеточный автомат выдаст $N_2 = 256$ различных последовательностей периода $T_2 = 124$, линейная сложность $LC_2 = 15$ и характеристический многочлен $P(x)^3$. Кроме того, автомат проходит несколько циклов повторяющиеся состояния формы: $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ с $a_j \in GF(2)$.

4. Если $A_3 \neq 0$, то клеточный автомат выдаст $N_3 = 8192$ различных последовательностей периода $T_3 = 124$, линейной сложности $LC_3 = 20$ и характеристического полинома $P(x)^4$. Кроме того, автомат циклически перебирает состояния, не входящие в предыдущие циклы.

В итоге, простая линейная структура, основанная на КА, позволяет нам последовательно совершать конкатенацию для вычисления всех решений линейных двоичных разностных уравнений, некоторые из которых будут являться псевдослучайными бинарными последовательностями.

Сравнение с алгоритмом использования векторных дополнительных и перестановочных операций. Клеточные автоматы используют разными способами для генерации псевдослучайных криптографических последовательностей. Существует метод, в котором модель клеточного автомата генерирует бинарную последовательность при помощи алгоритма использования векторных дополнительных и перестановочных операций для расширения пространства логических функций [10].

В данном алгоритме перестановки *n*-арных логических функций и дополнительного алгоритма перестановка выполняется для $2^n!$; дополнительные исчерпывающие потребности 2^{2^n} операций для каждой из операций перестановки. Суммарная вычислительная сложность n-мерного варианта логической функции с использованием перестановки и дополнительного алгоритма – $2^n! \times 2^{2^n}$.

Вышеупомянутые характеристики делают псевдослучайную двоичную последовательность, сгенерированную данным шифром возможным только для блочных шифров, а применение линейных клеточных автоматов имеет очевидное преимущество при потоковом шифровании в реальном времени.

Использование алгоритма в системах контроля целостности и аутентичности блочных данных. Предлагаемый алгоритм может быть использован как алгоритмическая основа для реализации программных или аппаратных систем контроля целостности и аутентичности не только потоковых, но и блоковых данных (рис. 1).

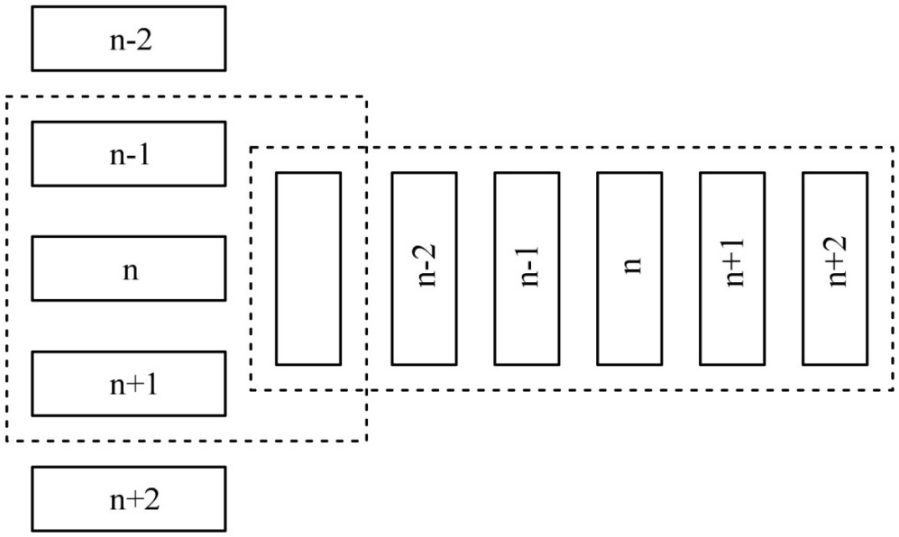


Рисунок 1 – Схема алгоритма контроля целостности и аутентичности данных для блоковых данных

Если рассматривать поток блочных данных от источника к приемнику, то модель системы контроля реализуется следующим образом. Источник поддерживает счетчик количества принятых блоков, для которых процедура дала положительный результат (в нашем случае n–1). Вектор сформированных с помощью предлагаемого подхода псевдослучайных блоков данных длиной $l = l_1 + l_2$, используемых для декодирования поступающего пакета:

$$V^n = \{V_{n-l_1}, ..., V_{n+l_2}\}, \; V_i = f(i, ключ) \; . \tag{10}$$

В данном случае, l_1 – параметр, определяющий, на какое максимальное число индекс поступающего информационного блока может быть меньше максимального индекса блоков, уже буферизированных к текущему моменту, чтобы может быть записанным в буфер; l_2 – показатель, показывающий, на какое максимальное число индекс поступающего информационного блока может превышать максимальный индекс блоков $n-1$, обработанных к текущему моменту. При этом равенство параметра l_1 единице будет означать невозможность для легальных информационных пакетов менять очередность поступления в приемник, так как в этом случае разница между индексами легальных информационных блоков, поступающих подряд в приемник, может иметь значение от 2 и более. Это увеличивает вероятность ошибки при передаче всего множества пакетов и накладывает высокие требования к протоколу связи, который должен гарантировать доставку блоков в исходном порядке. Все это потребует от системы связи буферизации, контроля очередности и выльется, в конечном счете, в снижение пропускной способности канала.

Поступающий информационных блок S проходит операцию декодирования для каждого из слов вектора:

$$F(S, V^n) = \{S_{n-l_1}, ..., S_{n+l_2}\} \; . \tag{11}$$

В составе каждого информационного блока в момент его формирования до операции закрытия в источнике добавлены контрольные разряды, формируемые любым методом контроля целостности и обнаружения ошибок.

Каждое из полученных в результате декодирования слов $S_{n-l_1}, ..., S_{n+l_2}$ проходит проверку на отсутствие ошибок:

$F^{err}(\widetilde{S}_{n-l_1}) = 1$, *если ошибок нет*

$F^{err}(\widetilde{S}_{n-l_1}) = 0$, *если ошибка*

В случае, если проверка ошибок для каждого слова дала 0, то поступивший пакет признается пакетом, сформированным не целевым, а посторонним источником. В случае, если проверка ошибок дала 1, для одного слова, то его индекс определяется как индекс поступившего пакета. В случае если проверка ошибок дала 1, для более чем одного слова, то произошла ошибка аутентификации.

Отличием предлагаемого метода является то, что затраты на его реализацию определяются размером вектора, с элементами которого сравнивается поступающее слово. А его размер, в свою очередь, определяется вероятностью возникновения ошибок в канале: чем она больше, тем большая длина вектора требуется для снижения вероятности ошибки непопадания индекса поступившего блока в диапазон $n-l_1 \ldots n+l_2$. Кроме того, для повышения производительности, элементы проверочного вектора можно формировать до момента получения пакета.

Выводы. В данной статье показано, что все решения линейных бинарных разностных уравнений могут быть реализованы с помощью линейных моделей на основе клеточных автоматов при использовании правил 90/150. Примечательно, что некоторые из этих решений имеют прямое криптографическое применение в шифрах, потому что они представляют собой последовательности ключевого потока, созданные с помощью псевдослучайных генераторов.

Также стоит отметить, что генераторы псевдослучайных последовательностей, задуманные и спроектированные как нелинейные генераторы, здесь линеаризованы на клеточных автоматах. Процедура линеаризации проста и может применяться в ряде практических криптографических решениях. Эта характеристика делает алгоритм пригодным для разработки систем, в которых актуально оперативное выполнение в реальном времени, например, в системах связи с высокой скоростью передачи.

Предложен алгоритм применения псевдослучайной последовательности в системах контроля целостности и аутентичности блочных данных.

Библиографический список

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

2. Марухленко А. Л. Комплексная оценка информационной безопасности объекта с применением математической модели для расчета показателей риска / А. Л. Марухленко, А. В. Плугатарев, М. О. Марухленко, М. А. Ефремов // Известия Юго-Западного государственного университета. – 2018. – Т. 8, № 4 (29). – С. 34–40.

3. Gollmann D. Clock-Controlled Shift Registers: A Review / D. Gollmann // IEEE Transactions on Selected Areas in Communications. – 1989. – Vol. 7, № 4. – pp. 525–533.

4. Марухленко А. Л. Программный модуль для оценки криптостойкости симметричных методов шифрования с использованием параллельных вычислений / А. Л. Марухленко, М. О. Марухленко, А. В. Плугатарев, В. П. Добрица // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : материалы II Всероссийской научно-практической конференции. – Курск : ЮЗГУ, 2018. – С. 33–38.

5. Марухленко А. Л. Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, М. Ю. Шашков // Известия Юго-Западного государственного университета. – 2020. – Т. 24, № 2. – С. 108–121.

6. Кулешова Е. А. Программа для многопоточного шифрования на базе клеточных автоматов / Е. А. Кулешова, А. Л. Марухленко, В. П. Добрица, М. О. Таныгин, Л. О. Марухленко // Свидетельство о регистрации программы для ЭВМ RU 2019664789, 13.11.2019. Заявка № 2019663418 от 29.10.2019. – Режим доступа: https://www.elibrary.ru/item.asp?id=41364754. – Заглавие с экрана. – Яз. рус. (дата обращения: 03.03.2021).

7. Марухленко А. Л. Анализ потенциальных уязвимостей и современных методов защиты многопользовательских ресурсов / А. Л. Марухленко, М. О. Марухленко, Е. Е. Конорева, М. О. Таныгин // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : материалы II Всероссийской научно-практической конференции. – Курск : ЮЗГУ, 2018. – С. 136–140.

8. Wolfram S. Statistical mechanics of cellular automata / S. Wolfram // Reviews of Modern Physics. – 1983. – Т. 55 (3). – P. 601–644.

9. Sirakoulis G. C. Hybrid DNA Cellular Automata for pseudorandom number generation / G. C. Sirakoulis // International Conference on High Performance Computing & Simulation (HPCS). – Madrid, Spain : IEEE, 2012. – P. 238–244.

10. Wan J. Permutation and Complementary Algorithm to Generate Random Sequences for Binary Logic / J. Wan, J. Zheng // Variant Construction from Theoretical Foundation to Applications. – 2019. – P. 237–245.

References

1. Marukhlenko A. L., Plugatarev A. V., Tanygin M. O., Marukhlenko L. O., Bobintsev D. O. Variant organizatsii mnogopotochnoy obrabotki konfidentsialnykh dannykh na baze kletochnykh avtomatov [A Variant of the Organization of Multithreaded Processing of Confidential Data Based on Cellular Automata]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Bulletin of the Southwest State University], 2019, vol. 23, no. 3, pp. 100–112.

2. Marukhlenko A. L., Plugatarev A. V., Marukhlenko L. O., Efremov M. A. Kompleksnaya otsenka informatsionnoy bezopasnosti obyekta s primeneniyem matematicheskoy modeli dlya rascheta pokazateley riska [Comprehensive Assessment of the Information Security of an Object Using a Mathematical Model for Calculating Risk Indicators]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Izvestiya of the Southwest State University], 2018, vol. 8, no. 4 (29), pp. 34–40.

3. Gollmann D., Chambers W. C. Clock-Controlled Shift Registers: A Review. *IEEE Transactions on Selected Areas in Communications*, 1989, vol. 7, no. 4, pp. 525–533.

4. Marukhlenko A. L., Marukhlenko L. O., Plugatarev A. V., Dobritsa V. P. Programmnyy modul dlya otsenki kriptostoykosti simmetrichnykh metodov shifrovaniya s ispolzovaniyem parallelnykh vychisleniy [Software Module for Evaluating the Cryptographic Strength of Symmetric Encryption Methods Using Parallel Computing]. *Infokommunikatsii i kosmicheskiye tekhnologii: sostoyaniye, problemy i puti resheniya : materialy II Vserossiyskoy nauchno-prakticheskoy konferentsii* [Infocommunications and Space Technologies: State, Problems and Solutions : Proceedings of the II All-Russian Scientific and Practical Conference]. Kursk, YUZGU, 2018, pp. 33–38.

5. Marukhlenko A. L., Plugatarev A. V., Tanygin M. O., Marukhlenko L. O., Shashkov M. Yu. Variant razgranicheniya dostupa k informatsionnym resursam na osnove neyavnoy autentifikatsii [Variant of Differentiation of Access to Information Resources Based on Implicit Authentication]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Izvestiya Bulletin of the Southwest State University], 2020, vol. 24, no. 2. pp. 108–121.

6. Kuleshova E. A., Marukhlenko A. L., Dobritsa V. P., Tanygin M. O., Marukhlenko L. O. Programma dlya mnogopotochnogo shifrovaniya na baze kletochnykh avtomatov [A Program for Multithreaded Encryption Based on Cellular Automata]. *Certificate of registration of a computer program RU 2019664789, 11/13/2019. Application No. 2019663418 dated October 29, 2019*. Available at: https://www.elibrary.ru/item.asp?id=41364754 (accessed 03.03.2021).

7. Marukhlenko A. L., Marukhlenko L. O., Konoreva E. E., Tanygin M. O. Analiz potentsialnykh uyazvimostey i sovremennykh metodov zashchity mnogopolzovatelskikh resursov [Analysis of Potential Vulnerabilities and Modern Methods of Protecting Multi-User Resources]. *Infokommunikatsii i kosmicheskiye tekhnologii: sostoyaniye, problemy i puti resheniya : materialy II Vserossiyskoy nauchno-prakticheskoy konferentsii* [Infocommunications and Space Technologies: State, Problems and Solutions : Proceedings of the II All-Russian Scientific and Practical Conference]. Kursk, YUZGU, 2018, pp. 136–140.

8. Wolfram S. Statistical Mechanics of Cellular Automata. *Reviews of Modern Physics*, 1983, vol. 55 (3), pp. 601–644.

9. Sirakoulis G. C. Hybrid DNA Cellular Automata for Pseudorandom Number Generation. *International Conference on High Performance Computing & Simulation (HPCS)*. Madrid, Spain, IEEE, 2012, pp. 238–244.

10. Wan J., Zheng J. Permutation and Complementary Algorithm to Generate Random Sequences for Binary Logic. *Variant Construction from Theoretical Foundation to Applications*, 2019, pp. 237–245.