УДК 681.3+681.5:007

ДИСКРЕТНЫЕ АВТОМАТЫ С ПСЕВДОСЛУЧАЙНЫМИ ПЕРЕХОДАМИ И ПОДСТАНОВОЧНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ИХ ОСНОВЕ

АЛИПОВ Н.В.

Описываются методы генерации шифра защиты на основе дискретных автоматов с псевдослучайными переходами из одного состояния в другое.

Известно, что для защиты информации при ее хранении и передаче в основном используются криптографические методы [1]: подстановки, перестановки и аддитивные. При подстановках буквы открытого текста по некоторому правилу (ключу) заменяются буквами шифротекста, причем буквы открытого текста и шифротекста могут принадлежать одному и тому же алфавиту либо различным. Подстановочные шифры разгадывать просто. В 1926 г. инженер Вернам предложил нераскрываемый шифр [2], идея которого состояла в том, что для каждой новой подстановки выбирался новый ключ (величина циклического сдвига замены буквы открытого текста на букву шифротекста). Если такой ключ выбирать случайным образом, то, как доказал Шеннон в 1949 г. [3], шифр является нераскрываемым. Однако в этом случае длина ключа становится соизмеримой с длиной открытого текста и наряду с шифротекстом необходимо передавать и ключ. Обмен ключами размером с шифротекст не всегда уместен. Поэтому чаще используют псевдослучайную последовательность, вырабатываемую датчиком псевдослучайных чисел. В этом случае ключом является начальное его значение.

Возможен и другой вариант решения этой проблемы: воспользоваться теорией дискретных автоматов [4]. Сформулируем основные требования к такому автомату:

– он должен иметь одно начальное (исходное) состояние и N конечных (N – количество символов входного алфавита);

– переход автомата из начального в i -е конечное состояние $\left(i=\overline{1,N}\right)$ осуществляется через промежуточные состояния;

– последовательность промежуточных состояний (маршрутов) выбирается псевдослучайным образом;

– каждому конечному состоянию соответствует некоторое множество маршрутов;

– каждый маршрут представляет вариант кодирования символа входного алфавита;

– маршруты i -го конечного состояния имеют неодинаковую длину (используется неравнозначное кодирование символов входного алфавита).

Примером такого дискретного автомата является устройство управления помехоустойчивого аналого-цифрового преобразователя [5]. Как известно, преобразователи подобного типа в условиях действия помех формируют цифровой код, эквивалентный аналоговой величине. Такие устройства управления имеют одно начальное состояние и N конечных, где $N=2^n$; n – разрядность преобразователя; начинают функционировать из начального состояния, а под действием помех в одно и то же конечное состояние приходят различными маршрутами; каждому маршруту соответствует своя комбинация выходного сигнала, который принимает одно из значений:

$$Y_j=\begin{cases}0, & \text{если } x_1 \le x_{э_j};\\ 1, & \text{если } x_1 > x_{э_j},\end{cases}$$

где $x_1=x+\zeta(t)$, x – аналоговый сигнал; $\zeta(t)$ – помеха; $x_{э_j}$ – эталонный сигнал, с которым сравнивается аналоговый сигнал x_1; Y_j – выходной сигнал автомата на j -м такте кодирования, $j=\overline{1,n}$ (см. аналого-цифровые преобразователи поразрядного уравновешивания). Преобразование аналогового сигнала в цифровой эквивалент в зависимости от проявления помех может окончиться на том или ином такте кодирования (в самом неблагоприятном случае оно оканчивается на n -м такте). Это порождает неравнозначные кодовые комбинации, образованные выходным сигналом автомата.

Поскольку $\zeta(t)$ – случайная функция, то выходной сигнал Y_j является случайной величиной. Следовательно, такие автоматы обеспечивают псевдослучайные переходы его из одного состояния в другое, формируют множество маршрутов различной длины из начального состояния в одно конечное.

Функционирование этих автоматов описывается помехоустойчивыми алгоритмами поиска точки с характерным признаком на отрезке единичной длины [5]. Результатами синтеза таких алгоритмов является ориентированный граф, задающий дискретный автомат [6], а количество его конечных состояний равно количеству полуоткрытых интервалов одинаковой длины, на которое разбивается исходный интервал неопределенности относительно точки с характерным признаком.

Естественно, возникает вопрос: каким образом использовать такой автомат в системах защиты информации? Для этой цели необходимо: выбрать

автомат, который имеет N конечных состояний; каждому символу входного алфавита поставить во взаимно-однозначное соответствие полуоткрытый интервал неопределенности, отождествленный с конкретным конечным состоянием. Следует заметить, что первый полуоткрытый интервал неопределенности соответствует первому конечному состоянию; второй – второму и т.д.; N-й символ входного алфавита соответствует последнему конечному состоянию.

Затем – выбрать виртуальный датчик (ДВП) физически несуществующих помех, сформировать на j-м такте функционирования автомата смесь такого вида:

$$x_j = x_\rho^1 + x_j^2, \qquad (1)$$

здесь x_ρ^1 – номер (число) конечного состояния, поставленного во взаимно-однозначное соответствие ρ-му символу входного алфавита, $\rho = \overline{1,N}$; x_j^2 – амплитуда виртуальной помехи, сформированной ДВП на j-м такте функционирования автомата, $j = \overline{1,n}$.

Смесь x_j подать на вход дискретного автомата и получить сигнал Y_j:

$$Y_j = \begin{cases} 0, & \text{если } x_j \le x_э; \\ 1, & \text{в противном случае,} \end{cases} \qquad (2)$$

где $x_э^j$ – эталонный цифровой эквивалент, формируемый дискретным автоматом на j-м такте.

Соотношения (1) формировать до достижения автоматом x_ρ^1-го конечного состояния. Совокупность выходных сигналов автомата

$$Y_1, Y_2, \ldots, Y_z; \quad z \le n \qquad (3)$$

представляет собой шифр замены ρ-го символа входного алфавита.

Поскольку выходной сигнал автомата на j-м такте его функционирования является случайной величиной, то и выбор определенного шифра замены из множества возможных осуществляется случайным образом.

Шифры замены являются кодовыми комбинациями префиксного (неравнозначного) кода, что существенно затрудняет их декодирование.

Итак, для получения шифра замены символа входного алфавита необходимо создать структуру, состоящую из датчика виртуальных помех, сумматора и дискретного автомата, реализующего один из алгоритмов помехоустойчивого поиска точки с характерным признаком в исходном интервале неопределенности.

Техническая реализация сумматора очевидна. Реализация ДВП и дискретного автомата связана со значительными трудностями, которые определяются особенностями их функционирования. Так, ДВП должен подавать на вход сумматора особые (хорошие) помехи, под действием которых автомат, переходя случайным образом из одного состояния в другое, в конце концов достиг бы конечного состояния, поставленного в соответствие кодируемому символу входного алфавита.

Дискретные автоматы подобного типа в какой-то мере являются фильтрами, осуществляющими подавление виртуальных помех алгоритмическими способами [5]. Алгоритмическое подавление помех эффективно только тогда, когда случайные возмущения можно описать параметрами [5]: амплитудой импульса (выброса), его длительностью и минимальным интервалом между двумя соседними выбросами. Каждый из этих параметров может быть случайной либо неслучайной величиной. Из этого следует: ДВП должен формировать только такие последовательности; они могут быть однополярными и двухполярными. В работе [5] они названы соответственно $A_1(a,l,H)$- и $A_2(a,l,H)$-последовательности (a – амплитуда выброса; l – длительность выброса; H – минимальный возможный интервал между двумя соседними выбросами).

Эти последовательности получают из псевдослучайных последовательностей чисел, равномерно распределенных в интервале $(0,1)$ [7].

Для организации псевдослучайных переходов дискретного автомата, как уже известно, используют помехоустойчивые алгоритмы поиска. Задача синтеза этих алгоритмов формулируется следующим образом [5]:

точка $x \in [x_{min}, x_{max}]$,

процесс поиска состоит из i шагов (тактов), на каждом шаге совершается один эксперимент, на процесс поиска накладывается виртуальная $A_\nu(a,l,H)$-последовательность, $\nu = 1,2$. В этих условиях требуется за i шагов однозначно заключить точку x в интервал неопределенности наименьшей длины.

Под экспериментом понимают проверку предиката:

$$Y_j = P\{x_j > x_э^j\}. \qquad (4)$$

При этом, если $P\{x_j > x_э^j\} = 0$, то $x \in [x_Л^{j-1}, x_э^j)$; если $P\{x_j > x_э^j\} = 1$, то $x \in [x_э^j, x_п^{j-1})$, где $[x_Л^{j-1}, x_п^{j-1})$ – полуоткрытый интервал неопределенности относительно точки x, выделенной на предыдущем шаге (исходным интервалом неопределенности является интервал (x_{min}, x_{max})).

Для алгоритмического подавления помех применяют принципы “пересечения” и “повторных сравнений” [5].

Поясним первый из них. Пусть на $(j-1)$-м шаге алгоритма относительно x выделен полуоткрытый интервал неопределенности $[x_Л^{j-1}, x_п^{j-1})$, на j-м шаге сформирован эталон $x_э^j$, на основании которого получено новое значение выходного сигнала

Y_j. Тогда формируем относительно x такие полуоткрытые интервалы неопределенности:

$$x \in \begin{cases} \left[x_{\Lambda}^{j-1}, x_{э}^{j,2}\right), Y_j = 0; \\ \left[x_{э}^{j,1}, x_{п}^{j-1}\right), Y_j = 1, \end{cases}$$

где $$x_{э}^{j,2} = \begin{cases} x_{э}^{j} + a, x_{э}^{j} + a \le x_{п}^{j-1}; \\ x_{п}^{j-1}, x_{э}^{j} + a > x_{п}^{j-1}, \end{cases}$$

$$x_{э}^{j,1} = \begin{cases} x_{э}^{j} - a, x_{э}^{j} - a \ge x_{\Lambda}^{j-1}; \\ x_{\Lambda}^{j-1}, x_{э}^{j} - a < x_{\Lambda}^{j-1}. \end{cases} \quad (5)$$

Для принципа "повторных сравнений" характерно то, что эксперимент повторяют на соседних шагах алгоритма (на них формируют один и тот же эталон).

Рассмотрим конкретный пример. Пусть процесс поиска состоит из i шагов, на каждом шаге совершается один эксперимент, $x \in [0, x_{max}]$, на процесс поиска накладывается $A_2(a,1,3)$-последовательность и на первом шаге алгоритма сформирован эталон $x_{э}^{1} \in [0, x_{max}]$. Тогда по итогам первого шага алгоритма на основании принципа "пересечения" формируем такие полуоткрытые интервалы:

$$x \in \begin{cases} \left[x_{\Lambda}^{0}, x_{э}^{1,2}\right), Y_1 = 0; \\ \left[x_{э}^{j,1}, x_{п}^{0}\right), Y_1 = 1. \end{cases}$$

Пусть на втором шаге алгоритма применяется принцип "повторных сравнений", для которого $x_{э}^{2} = x_{э}^{1}$ (можно применить и принцип "пересечения").

Тогда по итогам выполнения двух первых шагов получают такие комбинации выходных сигналов: 00; 01; 10; 11.

Для первой и четвертой комбинации характерно то, что на первых двух шагах алгоритма амплитуда виртуальной последовательности была равна нулю (по условию длительность выброса виртуальной последовательности равна длительности шага алгоритма) и результаты первых двух экспериментов достоверны.

Поэтому выделяем соответственно такие полуоткрытые интервалы неопределенности относительно точки x:

$$x \in \left[0, x_{э}^{1}\right); \; x \in \left[x_{э}^{1}, x_{max}\right] \quad (6)$$

и на последующих шагах алгоритма по такой же схеме размещаем в них эталонные значения.

Для второй и третьей комбинации характерно противоречие (для одного и того же эталона получены различные значения выходного сигнала), которое свидетельствует о действии виртуальной последовательности на первом либо на втором шаге алгоритма.

В такой ситуации на третьем шаге снова применяем принцип "повторных сравнений" (сохраняем эталон, $x_{э}^{3} = x_{э}^{1}$, можно применить и принцип "пересечения").

По итогам выполнения первых трех шагов алгоритма получаем такие комбинации выходных сигналов:

010; 011; 100; 101. (7)

Для первой и четвертой комбинации характерно действие виртуальной последовательности на втором шаге (см. условие задачи). Следовательно, результаты первого и третьего экспериментов достоверны. По этой причине выделяем по итогам выполнения третьего шага соответственно такие полуоткрытые интервалы: $x \in \left[0, x_{э}^{1}\right)$; $x \in \left[x_{э}^{1}, x_{max}\right]$.

По определению виртуальной последовательности ее проявление не будет наблюдаться по крайней мере еще на четвертом и пятом шагах алгоритма. На этих шагах применяют классический алгоритм поиска (дихотомию), посредством которого выделенные полуоткрытые интервалы неопределенности будут разбиты за два шага на четыре части. После выполнения пятого шага алгоритма к выделенному интервалу неопределенности относительно точки x применяют описанную на первых трех шагах схему формирования эталонов.

Для второй и третьей комбинации характерно то, что виртуальная последовательность действовала на первом шаге, на втором и третьем шагах ее проявление не наблюдалось. По определению $A_2(a,1,3)$-последовательности оно не будет наблюдаться и на четвертом шаге алгоритма. На этом шаге на полуоткрытых интервалах $\left[x_{э}^{1}, x_{max}\right)$, $\left[0, x_{э}^{1}\right)$ применяют классический алгоритм поиска, посредством которого они будут разбиты на две равные части. После выполнения четвертого шага алгоритма к вновь выделенному полуоткрытому интервалу неопределенности относительно точки x применяют описанную на первых трех шагах схему формирования эталонов.

Предположим, что описанный алгоритм поиска за i шагов разбивает исходный интервал неопределенности на $\varphi(i,1)$ равные части, за $(i-1)$ шаг – на $\varphi(i-1,1)$ равные части и т.д. Тогда полуоткрытые интервалы (6) будут разбиты на $\varphi(i-2,1)$ равные части (для их выделения было истрачено два шага алгоритма).

Полуоткрытые интервалы неопределенности, соответствующие первой и четвертой комбинации последовательности (7), будут первоначально разбиты на четыре части каждый, затем каждый вновь выделенный интервал неопределенности будет разбит на $\varphi(i-5,1)$ равные части (в распоряжении алгоритма осталось $(i-5)$ шагов).

Полуоткрытые интервалы неопределенности, соответствующие второй и третьей комбинации последовательности (7), будут разбиты первоначально на две части, затем каждый вновь выделенный интервал неопределенности будет разбит на $\varphi(i-4,1)$ равные части.

Поскольку $l([0, x_{max}]) = l([0, x^1_э]) + l([x^1_э, x_{max}])$, где $l([a, b])$ – длина отрезка $[a, b]$, то справедливыми будут соотношения:

$$x^1_э = \min\{\varphi(i-2,1), 4\varphi(i-5,1), 2\varphi(i-4,1)\}; \quad (8)$$

$$\varphi(i,1) = 2\min\{\varphi(i-2,1), 4\varphi(i-5,1), 2\varphi(i-4,1)\}.$$

Запишем очевидные соотношения:

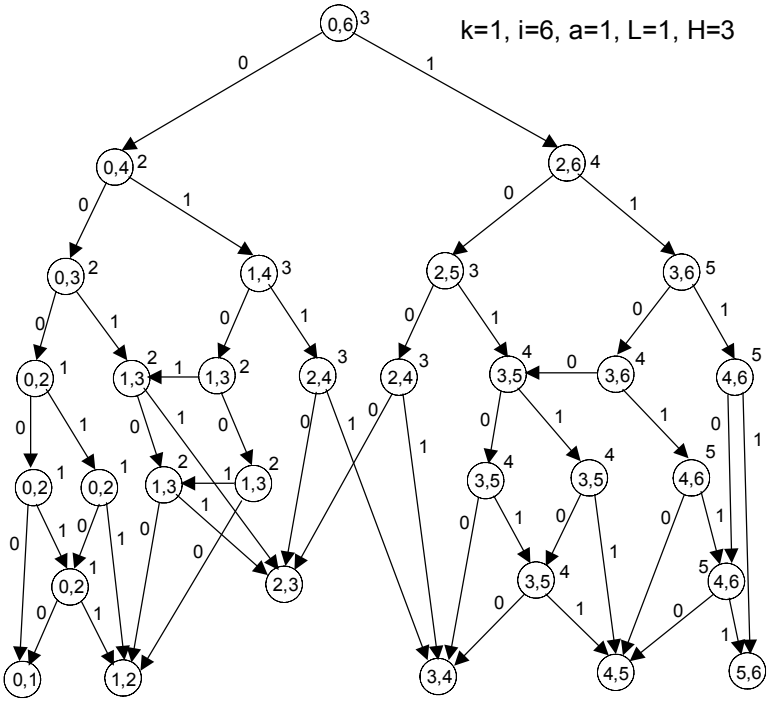
$$\varphi(1,1) = \varphi(2,1) = 1; \ \varphi(3,1) = 2. \quad (9)$$

Выражения (8), (9) по схеме принципа "повторных сравнений" методом индукции позволяют построить алгоритм поиска для любых его параметров и параметров виртуальной последовательности.

На рисунке приведен ориентированный граф одного из таких алгоритмов, который синтезирован для условий: $x \in [0,6]$, $i = 6$, $a = 1$, $l = 1$, $H = 3$.

Внутри вершины (рисунок) записан исходный интервал неопределенности, рядом с вершиной – эталонное значение, на ребрах графа приведены значения выходного сигнала.

Используя данный алгоритм, синтезируют дискретный автомат, который имеет шесть конечных состояний; для каждого из них существует множество маршрутов из начального состояния; маршруты имеют различную длину; их выбор осуществляется псевдослучайным образом. Следовательно, такой автомат в совокупности с сумматором и ДВП может генерировать шифры замены для шестиричной позиционной системы.



Оптимальный помехоустойчивый алгоритм поиска, преобразования информации, подавляющий A_2-последовательность

Очевидным является тот факт, что количество маршрутов из начального состояния в одно и то же конечное состояние возрастает с увеличением амплитуды выброса виртуальной последовательности. Для нашего примера при амплитуде выброса, равной единице, количество маршрутов достигает семи для второго, третьего, четвертого и пятого конечных состояний и трех – для первого и шестого состояний.

Следует заметить, что для одних и тех же исходных данных (количество конечных состояний и параметров виртуальной помехи) существует множество помехоустойчивых алгоритмов поиска. Алгоритмы друг от друга отличаются выбором эталонных значений на каждом шаге; стратегией поиска (используется принцип "пересечения" либо принцип "повторных сравнений", либо их комбинация); правилами формирования нового интервала неопределенности; комбинацией классического (дихотомии) и помехоустойчивого алгоритмов.

Многообразие алгоритмов помехоустойчивого поиска, сложность задачи их синтеза, псевдослучайный способ формирования шифра замены, являющегося кодовой комбинацией префиксного кода, вносят значительную неопределенность и, тем самым, усложняют процесс декодирования шифротекста.

Литература: 1. *Спесивцев А.В., Вегнер В.А. и др.* Защита информации в персональных ЭВМ. М.: Радио и связь, 1992. 191 с. 2. *Vernam B.S.* Cipher printing telegraph systems for secret wire and radio telegraphie communication // Amer. just. electr. eng. 1926. Vol.45. N2. P.109-115. 3. *Шеннон К.* Теория связи в секретных системах // Шеннон К. Работы по теории информатики и кибернетике: Пер. с англ. М.: Иностр. лит., 1963. 310 с. 4. *Ecker A.* Abctrakte kriptographische Mashinen // Angew. Informatik. 1975. Bol.17, Nr 5. S.201-205. 5. *Алипов Н.В.* Разработка теории и методов решения задач помехоустойчивого поиска и преобразования информации // Автореф. дис. на соиск. уч. степени д-ра техн. наук. Харьков: ХИРЭ, 1986. 50 с. 6. *Арифметика*, принципы организации диагностики и формализованного проектирования вычислительных структур и устройств / В.П. Тарасенко, Н.В. Черкасский, Н.В. Алипов и др. К.:Вища шк., 1989. 343 с. 7. *Алипов Н.В., Алипов И.Н., Булах Е.В., Охапкин А.А., Ребезюк Л.Н.* Датчики виртуальных помех, используемые для организации функционирования дискретных автоматов в системах защиты информации // Радиотехника. 1999. Вып.111. С. 33-39.

Поступила в редколлегию 17.05.2001

Рецензент: д-р техн. наук Руденко О.Г.

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-94.