УДК 681.3+681.5:007

СТРУКТУРА ДИСКРЕТНЫХ АВТОМАТОВ С ПСЕВДОСЛУЧАЙНЫМИ ПЕРЕХОДАМИ

АЛИПОВ И.Н., БУЛАХ Е.В., РЕБЕЗЮК Л.Н.

В работе [1] обосновано новое направление в развитии криптографических методов защиты информации: использование ДА с псевдослучайными переходами из одного состояния в другое. Это позволяет формировать псевдослучайным образом подстановки для символов входного алфавита. В работе [2,3] синтезированы алгоритмы функционирования таких ДА. В данной работе рассматривается структура их организации.

Для того чтобы определить структуру дискретных автоматов (ДА) подобного класса, необходимо выявить особенности функционирования устройств поиска точки экстремума унимодальной функции. К этим особенностям следует отнести унимодальность функции; способ ее формирования; процедуру смещения точки экстремума в исходном интервале неопределенности; способ выделения максимального (минимального) значения этой функции в точках эксперимента, выполненного на каждом шаге алгоритма; способ реализации ДА, задаваемого логической схемой алгоритма; процедуру формирования смеси координаты точки экстремума функции с импульсами виртуальной последовательности.

Исходными данными являются: значение координаты точки экстремума унимодальной функции; вид и параметры виртуальной последовательности. Следует заметить, что ДА в результате своей работы координату точки экстремума, представленную в двоичной или десятичной системе, преобразует в неравнозначный код (выбирает под действием виртуальной последовательности из множества подстановок для конкретного двоичного и десятичного числа псевдослучайным образом одну из них). Одна из возможных структур ДА с псевдослучайными переходами для случая, когда унимодальная функция формируется аналоговым способом, представлена на рисунке. Эта структура включает в себя блоки: П – передатчик; A_1 – обычный дискретный автомат, реализующий один из алгоритмов поиска точки экстремума унимодальной функции; УСР – устройство сравнения аналоговых сигналов $f(x_1^j)$, $f(x_2^j)$, $f(x_3^j)$, где j – номер шага алгоритма поиска; $УСч_1$, $УСч_2$, $УСч_3$ – устройства считывания аналогового значения функции в точках x_1^j, x_2^j, x_3^j; Φ_1, Φ_2, Φ_3 – формирователи унимодальной функции, экстремум которой находится в точке x^*; Σ – аналоговый сумматор, на вход которого поступает координата точки экстремума и импульсы виртуальной последовательности; ДВП – датчик виртуальной последовательности, на вход которого поступают параметры виртуальной последовательности a, l, H.

Структура функционирует следующим образом: импульсом начальная установка "НУ" схема устанавливается в исходное состояние ($ДА_1$ – в начальное состояние); затем посредством блока Σ импульсы виртуальной последовательности аддитивно накладываются на координату точки экстремума x^*.

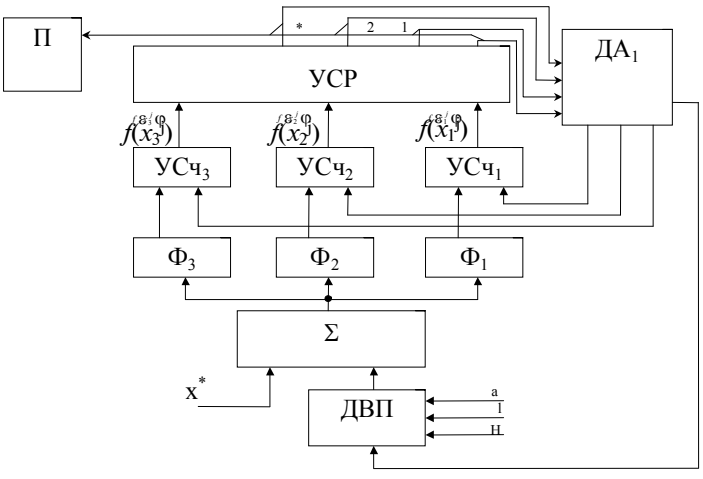
Потом эта аддитивная смесь подается на формирователи Φ_1, Φ_2, Φ_3, которые генерируют унимодальную функцию в точке экстремума $x^* + \xi$, где ξ – импульсы виртуальной последовательности. Блоки $УСч_1$, $УСч_2$, $УСч_3$ осуществляют считывание значений унимодальной функции в точках x_1^1, x_2^1, x_3^1, которые формирует $ДА_1$. Блок УСР выделяет максимальное значение функций из трех значений, сформированных блоками $УСч_1$, $УСч_2$, $УСч_3$.

На выходе блока УСР появляется один из сигналов "0", "1", "2", "*" :

$$Y\rho_1 = \begin{cases} 0, & f(x_1^1) = \max_{\rho} f(x_\rho^1); \\ 1, & f(x_2^1) = \max_{\rho} f(x_\rho^1); \\ 2, & f(x_3^1) = \max_{\rho} f(x_\rho^1); \\ *, & \text{если шаг пропускается}; \end{cases} \quad \text{где } \rho = \overline{1,2,3}.$$

Сигнал Y_1 поступает на вход передатчика П и $ДА_1$. Под воздействием сигнала Y_1 $ДА_1$ переходит в следующее состояние, и структура продолжает функционировать аналогичным образом. Процесс выбора подстановки прекращается в тот момент, когда $ДА_1$ достигает одного из конечных состояний, затем таким же образом выбирается подстановка для следующего значения координаты точки. Следует заметить, как только $ДА_1$ переходит в новое состояние, ДВП формирует новое значение виртуальной последовательности.

Из функционирования структуры, изображенной на рисунке, следует, что дискретный автомат с псевдослучайными переходами включает в себя обычный дискретный автомат $ДА_1$ и специальную схему для организации псевдослучайных переходов, в которую входят: ДВП, Σ, Φ_1, Φ_2, Φ_3, $УСч_1$, $УСч_2$, $УСч_3$, УСР.



Возможна и другая структура, в которой формирование унимодальной функции выполняется на дискретных элементах. В этой структуре значения унимодальной функции запоминаются, к примеру, в ПЗУ, причем в нем записывается только стандартная функция, т.е. функция, имеющая экстремум в нулевой точке; значения точек экстремума отождествляются с адресами ПЗУ. Так, если символов внешнего алфавита будет 64, амплитуда виртуальной последовательности не более 64, то для этой цели следует использовать ПЗУ с параметрами 512*8. В этом случае исходному интервалу неопределенности [0,1] будут соответствовать адреса ПЗУ (ОЗУ), начиная с 257 и кончая 384. В двух соседних ячейках ПЗУ, начиная с 257, 258 и т.д., будет записано одно и то же значение унимодальной функции. Этот прием позволяет исключить дополнительные состояния ДА. Затем стандартная функция преобразуется в другую функцию для любой другой точки экстремума таким образом.

Пусть координата точки экстремума равна N_{x^*}. Тогда для получения унимодальной функции (координата точки экстремума которой равна N_{x^*}) необходимо информацию с ПЗУ перезаписать в ОЗУ по такому правилу: информацию из ячейки ПЗУ A_1 записать в ячейку ОЗУ $[A_1 + 2N_x + 1]$. Поскольку аргумент унимодальной функции есть аддитивная смесь координаты точки экстремума и амплитуды импульса виртуальной помехи, то запись из ПЗУ в ОЗУ осуществляется по другой форме: информация из ячейки ПЗУ A_1 записывается в ячейку ОЗУ $[A_1 + 2N_x + 1 + \xi]$, где ξ – амплитуда импульса виртуальной помехи.

После того, как функция сформирована, выполняют последовательно чтение информации из ячеек:

$$B_1 = 256 + 2[A_1^j + 1],$$

$$B_2 = 256 + 2[A_2^j + 1],$$

$$B_3 = 256 + 2[A_3^j + 1].$$

Затем устройством сравнения будет сформирован, как уже известно, один из сигналов "0", "1", "2", "*", которые поступают на входы $ДА_1$ и передатчик. Дискретный автомат переходит в другое состояние. В дальнейшем такая структура функционирует аналогичным образом.

Из ДА с псевдослучайными переходами можно организовать различные последовательные их объединения. Такие совокупности ДА с псевдослучайными переходами строят следующим образом. Пусть входной алфавит содержит 64 символа. Тогда все эти символы разобьем на восемь групп, каждая из которых содержит восемь символов входного алфавита. Для псевдослучайного выбора подстановок в этом случае необходимо иметь два ДА: один ДА кодирует номер группы, другой – номер символа в группе. Функционирует такое объединение по следующей схеме: первоначально работает первый автомат, формируя подстановку номеру группы символов и переходя псевдослучайным образом из начального состояния в конечное. Как только первым ДА будет достигнуто конечное состояние, в работу вступает второй ДА, переходя псевдослучайным образом из одного начального состояния в конечное, соответствующее номеру символа входного алфавита в выделенной группе. Этим самым совокупность выходных сигналов УСР образует псевдослучайную подстановку номеру символа входного алфавита в выделенной группе; после достижения конечного состояния вторым ДА совокупность ДА переходит в исходное состояние; система в дальнейшем функционирует аналогичным образом.

Структура декодирующего устройства проста: она содержит приемник и дискретный автомат типа $ДА_1$, соединенные последовательно. Эта структура функционирует следующим образом: принятые приемником сигналы $Y_1, Y_2, ..., Y_i$ последовательно поступают на вход $ДА_1$, который первоначально находился в исходном состоянии. Под воздействием этих сигналов $ДА_1$ переходит из начального в одно конечное состояние, соответствующее принятому символу входного алфавита. После достижения конечного состояния $ДА_1$-м он переходит в начальное состояние, и следующий принятый сигнал Y_j считается первым сигналом второго принятого символа входного алфавита. Такая особенность ДА с псевдослучайными переходами позволяет без разделителей декодировать неравнозначные кодовые комбинации псевдослучайных подстановок. Этим самым достигается повышение быстродействия устройств декодирования.

Рассмотренная структура ДА с псевдослучайными переходами из одного состояния в другое позволяет на своей основе создавать аппаратные средства защиты информации при ее передаче.

Литература: 1. *Алипов И.Н., Ребезюк Л.Н.* Постановка задач синтеза новых методов защиты информации // Радиотехника. 1997. Вып. 103. С. 60-64. 2. *Булах Е.В.* Методы защиты информации на основе деревообразных автоматов / Зб. наукових праць за матеріалами 3-го міжнародного молодіжного форуму "Радіоелектроніка і молодь у XXI ст.", ч. 2. Харків: ХТУРЕ, 1999. 502 с. 3. *Алипов Н.В., Булах Е.В.* Синтез помехоустойчивых к нерегулярным возмущениям алгоритмов поиска точки экстремума унимодальной функции // Радиоэлектроника и информатика. 1999. № 3. С. 66-89.

Поступила в редколлегию 19.10.99

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

Алипов Илья Николаевич, канд. техн. наук, научный сотрудник ХТУРЭ. Научные интересы: защита информации. Адрес: Украина, 61189, Харьков, ул. Иртышская, 8, тел. 40-94-94.

Булах Евгений Вячеславович, аспирант кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации. Адрес: Украина, 61007, Харьков, пр.50 лет ВЛКСМ, 65-а, кв. 8, тел. 40-94-94.

Ребезюк Леонид Николаевич, канд. техн. наук, доцент кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации, автоматизация проектирования электронных вычислительных средств. Адрес: Украина, 61136, Харьков, ул. Ком. Уборевича, 40-б, кв. 17, тел. 69-79-38.