УДК 004.4:681.3

В.П. Семеренко

Винницкий национальный технический университет, Винница

РЕКОНСТРУКЦИЯ ЛИНЕЙНЫХ СКРЕМБЛЕРОВ НА ОСНОВЕ АВТОМАТНЫХ МОДЕЛЕЙ

Предлагается теория линейной последовательностной схемы (ЛПС) для представления скремблеров и поточных шифров, которые используют сдвиговые регистры. Рассмотрена модель функционирования аддитивного и самосинхронизирующего скремблеров на основе математического представления симметрии времени. Показан способ восстановления с линейной сложностью в обратном порядке неизвестной псевдослучайной последовательности по ее известному r-битовому фрагменту с помощью r-мерной ЛПС.

Ключевые слова: *скремблеры, криптография, поточное шифрование, линейные последовательностные схемы, время, обратный автомат.*

Введение

В современной цифровой технике широко используется скремблирование (scramble – перемешивание) – обратимое преобразование структуры цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности [1]. Области применения скремблеров – телефонные сети общего пользования, спутниковая и радиорелейная связь, цифровое телевидение.

Основная цель скремблирования состоит в повышении надежности синхронизации устройств на стороне передатчика и приемника с помощью улучшения статистических свойств, передаваемых данных. В результате скремблирования на стороне приемника изменяется вид информационной последовательности I, т.е. происходит шифрование открытого текста. С помощью дескремблера на стороне приемника последовательность I восстанавливается, т.е. дешифрируется. Таким образом, мы имеем дело с разновидностью потокового шифрования. Благодаря высокой скорости преобразований такое шифрование наиболее пригодно для мобильной и других видов связи. Поэтому актуальным является совмещение операций скремблирования и защиты информации.

Целью работы является изучение криптографических свойств различных типов скремблеров на основе математического аппарата линейных последовательностных схем и временных моделей.

Постановка задачи. Линейное скремблирование и потоковое шифрование базируются на использовании псевдослучайной последовательности (ПСП), которую может генерировать регистр сдвига с линейной обратной связью (РСЛОС). Для получения ПСП максимальной длины (М-последовательности), равной 2^r-1, структуру обратных связей (ОС) r-разрядного РСЛОС должен определять примитивный полином.

Преимуществами РСЛОС являются хорошие криптографические свойства М-последовательности и легкость алгебраических преобразований. С другой стороны, поточный шифр только на основе РСЛОС считается криптографически слабым и поэтому к нему обычно добавляется схема, реализующую нелинейную функцию [2].

Поскольку в большинстве поточных шифров базовым элементом по-прежнему является РСЛОС, поэтому остается пристальный интерес к его изучению. Важной научно-технической задачей является задача реконструкции, т.е. восстановления неизвестных параметров скремблеров на основе РСЛОС по другим параметрам [3, 4].

Рассмотрим возможные способы решения этой задачи для двух типов скремблеров: аддитивных и самосинхронизирующих.

Для характеристики скремблирования и потокового шифрования на основе РСЛОС обычно используются следующие параметры:

– разрядность (длина) r РСЛОС;

– структура ОС (полином ОС);

– начальное состояние $S(0)$ РСЛОС;

– информационная последовательность I;

– псевдослучайная последовательность X;

– скремблированная последовательность Z.

Все последовательности имеют длину n.

На практике некоторые из перечисленных параметров могут быть выражены через другие. Сложность определения одних, неизвестных, параметров через другие, известные, может определить степень криптостойкости скремблера.

Как правило, известной для всех является последовательность Z, а неизвестной – последовательность X или I. Для восстановления неизвестных последовательностей криптоаналитику необходимо знать некоторую дополнительную информацию об РСЛОС: либо структуру ОС, либо начальное состояние $S(0)$, либо фрагмент открытого и зашифрованного текста.

Неизвестную аппаратную структуру РСЛОС можно определить с помощью $2r$ бит открытого и

зашифрованного текста, либо с помощью алгоритма Берлекэмпа-Месси построить другой РСЛОС для генерации той же последовательности Z [5]. Недавно был предложен алгоритм для восстановления полинома ОС, используя только скремблированные биты [3].

На практике не всегда возможно или целесообразно удерживать в секрете аппаратную структуру РСЛОС. Можно значительно повысить криптозащищенность скремблированного текста даже при известной аппаратной структуре РСЛОС, если в качестве секретного ключа использовать начальное состояние S(0) РСЛОС. Именно нахождение S(0) и является главной целью многочисленных криптоатак.

Эффективной защитой от силовых атак полного перебора является выбор РСЛОС достаточно большой длины, не менее 100. Для защиты от другий типов атак не следует пренебрегать различными практическими рекомендациями по выбору полинома ОС. Например, легко раскрываются криптогенераторы с сильно разреженной структурой ОС [6].

Однако, несмотря на достигнутые успехи по взламыванию линейных криптосистем, еще имеется много нерешенных вопросов. Открытой проблемой остается нахождение эффективного алгоритма реконструкции скремблера, чья сложность существенно не зависит от веса полинома ОС [3]. Многие методы криптоанализа, разработанные для синхронных скремблеров, сложно применить для самосинхронизирующих скремблеров.

Изложение основного материала

Математические модели линейных скремблеров. Поскольку в основе линейных скремблеров используется РСЛОС, поэтому рассмотрим подробно его структуру. Учитывая тот факт, что РСЛОС является также основным схемотехническим узлом кодеров и декодеров циклических кодов, обратимся к математическим основам этих кодов.

Наиболее распространенным способом описания РСЛОС в помехоустойчивом кодировании является его порождающий полином

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{r-1} x^{x-1} + g_r x^r \quad . \quad (1)$$

Для решения нашей задачи целесообразно рассматривать РСЛОС как автомат линейного типа, известного также под названиями “линейная последовательностная схема” (ЛПС) или “линейная последовательностная машина” (ЛПМ) [7]. Более удачным является первый термин, который и будем далее использовать. Согласно [7], ЛПС с l входами, m выходами и r элементами памяти (ЭП) в дискретные моменты времени t задается функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2), \quad (2)$$

и функцией выходов

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2), \quad (3)$$

где $A = \left[a_{ij}\right]_{r \times r}$, $B = \left[b_{ij}\right]_{r \times l}$, $C = \left[c_{ij}\right]_{m \times r}$, $D = \left[d_{ij}\right]_{m \times l}$ – характеристические матрицы ЛПС, $S(t) = \left[s_i\right]_r$ – слово состояния, $U(t) = \left[u_i\right]_l$ – входное слово, $Y(t) = \left[y_i\right]_m$ – выходное слово.

Матрица A определяет внутреннюю сеть ЛПС, т.е. соединения между собой элементов памяти (ЭП). Матрица B определяет структуру входов ЛПС, а матрицы C и D – структуру ее выходов.

Будем использовать следующие два типа ЛПС.

1. *Рекурсивные ЛПС типа Фибоначчи* – это ЛПС, у которых матрицы A и B имеют вид

$$A = \begin{vmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \cdots & 1 \\ g_0 & g_1 & g_2 & \ldots & g_{r-1} \end{vmatrix}; \; B = \begin{vmatrix} 0 \\ 0 \\ \ldots \\ 0 \\ 1 \end{vmatrix}. \quad (4)$$

2. *Рекурсивные ЛПС типа Галуа* – это ЛПС, у которых матрицы A и B имеют вид:

$$A = \begin{vmatrix} 0 & 0 & 0 & \ldots & g_0 \\ 1 & 0 & 0 & \ldots & g_1 \\ 0 & 1 & 0 & \ldots & g_2 \\ \ldots & \ldots & \ldots & \cdots & \ldots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix}; \; B = \begin{vmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{vmatrix}. \quad (5)$$

Элементы последней строки матрицы A из (4) и элементы последнего столбца из (5) представляют собой коэффициенты полинома (1).

РСЛОС является простейшей аппаратной реализацией ЛПС. РСЛОС с сумматорами между отдельными ЭП – это ЛПС типа Галуа, а при отсутствии сумматоров между отдельных ЭП – тогда это ЛПС типа Фибоначчи.

Представление скремблеров с помощью характеристических матриц ЛПС определяет их автоматно-аналитическую модель [8].

Если использовать автоматную диаграмму переходов (ДП) и диаграмму выходов (ДВ) ЛПС, тогда можно получить автоматно-графовую модель скремблера [8, 9].

Для r-мерной ЛПС над полем GF(2) ДП представляет собой ориентированный граф $G_{FA}(V_{FA}, E_{FA})$, в котором 2^r вершин из множества вершин V_{FA} соответствуют 2^r внутренним состояниям автомата, а дуги из множества дуг E_{FA} показывают направления переходов между внутренними состояниями. В общем случае из вершины v_j ($v_j \in V_{FA}$) может выходить нулевая дуга и единичная дуга, а также могут входить нулевая дуга и единичная дуга.

Похожую графовую структуру имеет ДВ ЛПС.

Рассмотрим подробнее автоматную модель аддитивного скремблера.

Задачей такого скремблера является генерирование псевдослучайной последовательности X

максимальной длины (М-последовательности), которая в качестве гаммы накладывается на информационную последовательность I.

$$Z = I + X, \quad GF(2).$$

Напомним, что для получения с помощью ЛПС М-последовательности ее порождающий многочлен (1) должен быть примитивным и ЛПС после установки в некоторое начальное состояние $S(0)$ далее должна работать при нулевых входных воздействиях, т.е. в автономном режиме.

Автономная ЛПС имеет нулевые матрицы C и D, следовательно, ее работа может быть записана функцией состояний (переходов)

$$S(t+1) = A \times S(t), \quad GF(2) \qquad (6)$$

и функцией выходов

$$Y(t) = C \times S(t), \quad GF(2). \qquad (7)$$

Функционирование самосинхронизирующего скремблера зависит от входных воздействий, поэтому его автоматно-аналитической моделью является обычная ЛПС с функциями (2) и (3).

Анализ вычислительных процессов на основе симметрии времени. Если рассматривать категорию времени только с позиций математики, то можно заметить, что фундаментальные законы и классической, и квантовой динамики подразумевают эквивалентность причин и следствий, что влечет за собой эквивалентность “прошлого” и “будущего” [10]. Другими словами, теоремы, которые справедливы при изменении времени от “настоящего” в “будущее”, будут также справедливы при изменении времени от “настоящего” в “прошлое”.

Будем рассматривать динамические системы (ДС), которые характеризуются множествами входов, выходов и состояний, а также двумя функциями: переходов и выходов.

Ограничимся только интегрируемыми ДС с одной степенью свободы, для которых последовательность смен состояний во времени образует в пространстве состояний системы замкнутую фазовую траекторию в виде окружности [11].

Пусть на этой фазовой траектории будет начальное состояние S_{beg} и заключительное состояние S_{end}. В общем случае их взаимное расположение различно, следовательно, длина пути от S_{beg} к S_{end} по окружности в разные стороны будет различной. Обычно движение по фазовой траектории направлено вдоль точек (состояний), которые соответствуют моментам времени в порядке их возрастания, т.е. от “настоящего” в “будущее”. С позиций математики не существует запрета движения в обратном направлении. Если интерпретировать движение по циклической фазовой траектории от состояния S_{beg} в разные стороны как одновременное движение в противоположных временных направлениях, тогда можно рассмотреть задачу выигрыша во времени за счет выбора более короткого пути от S_{beg} к S_{end} (рис. 1).

Наиболее распространенным представителем таких ДС являются автономные конечные автоматы, в частности, автономные ЛПС. Как и в [12], будем рассматривать прямую и обратную автономные ЛПС.

Прямая автономная ЛПС – это обычная автономная ЛПС, которая описывается функциями (6) и (7). Для обратной автономной ЛПС аналогичные функции имеют вид:
функция переходов

$$S(t) = A_{inv} \times S(t+1), \quad GF(2), \qquad (8)$$

и функция выходов

$$Y(t) = C \times S(t), \quad GF(2). \qquad (9)$$

Для описания функционирования обратной автономной ЛПС достаточно иметь лишь матрицу A_{inv}. В [13] показаны правила перехода от матрицы A к матрице A_{inv}, и наоборот. Например, для матрицы A вида (4) матрица A_{inv} имеет вид:

$$A_{inv} = \begin{vmatrix} g_1 & g_2 & \cdots & g_{r-1} & g_0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \cdots & \ldots \\ 0 & 0 & \ldots & 1 & 0 \end{vmatrix}.$$

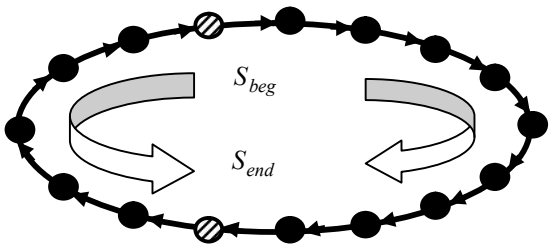

Рис. 1. Направления движения по фазовой траектории для автономной ЛПС

Реконструкция аддитивных скремблеров. Как уже отмечалось, математически операция аддитивного скремблирования состоит в побитовом сложении последовательностей I и X по правилам двоичного поля Галуа $GF(2)$. Рассмотрим классическую задачу криптоанализа по востановлению неизвестной псевдослучайной последовательности X по известных структуре ЛПС и скремблированной последовательности Z (рис. 2).

Поскольку генератор ПСП аддитивного скремблера является автономной ЛПС, поэтому для его описания можно перейти к функциям (6) – (9).

Традиционная задача криптоанализа такого автомата состоит в нахождении начального состояния $S(0)$ ЛПС, после чего восстанавливается искомая последовательность X. Такая задача основана на временных вычислениях от “настоящего” в “будущее”.

Рассмотрим восстановление последовательности X ЛПС, двигаясь во времени назад, в “прошлое”. Началом такого движения является конечное

состояние $S(n)$, в которое переходит ЛПС после подачи на нее последовательности X.

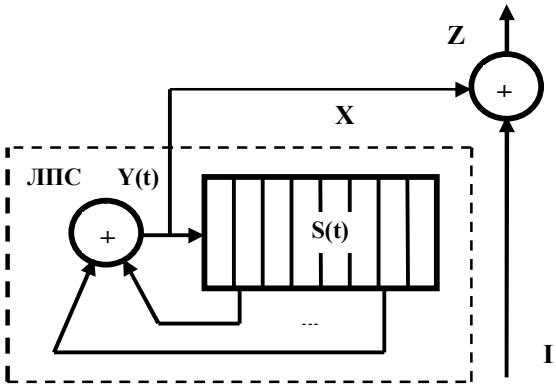

Рис. 2. Аддитивный скремблер на основе ЛПС типа Фибоначчи

Для нахождения r-битового слова состояния $S(n)$ необходимо в поле $GF(2)$ решить систему из r уравнений, которая следует из (3):

$$\begin{cases} y(n-r+1) = C \times S(n-r+1); \\ y(n-r+2) = C \times S(n-r+2); \\ \dots \\ y(n) = C \times S(n), \end{cases} \qquad (10)$$

где $y(n), \dots, y(n-r+1)$ – r-битовое слово, равное последним r битам последовательности X.

Отметим, что слова состояний $S(n-r+1), S(n-r+2), \dots, S(n)$ являются сдвинутыми копиями друг друга, поэтому в (10) мы имеем дело с одним неизвестным состоянием $S(n)$.

Решение системы уравнений (10) необходимо как для ЛПС типа Фибоначчи, так и типа Галуа. Единственным исключением является ЛПС типа Фибоначчи, у которой последовательность X поступает только с выхода последнего ЭП. В этом случае нет необходимости решать систему уравнений (10), поскольку последние r бит последовательности X непосредственно являются последним состоянием $S(n)$. Поэтому такой скремблер имеет минимальную криптозащиту.

После того, как будет получено состояние $S(n)$, далее по формулам (8) и (9) в обратном порядке до $S(0)$ восстанавливаются все предыдущие слова состояний ЛПС и, одновременно, соответствующие разряды последовательности X.

Аналогичным образом можно по любым известным r последовательным битам $x(i-r+1), x(i-r+2), \dots, x(i)$ последовательности X восстановить соответствующее слово состояниея $S(i)$ ЛПС, а затем, двигаясь вперед и назад во времени от состояния $S(i)$, восстановить с линейной сложностью всю псевдослучайную последовательность X. Для обеспечения такой возможности достаточно иметь r бит открытой и скремблированной информации.

Реконструкция самосинхронизирующихся скремблеров. Аддитивные скремблеры на основе автономных ЛПС работают при нулевых входных воздействиях, поэтому они являются линейными автоматами Мура. Функционирование самосинхронизирующих скремблеров зависит от поступающего на их вход информационной последовательности I, что позволяет отнести такие скремблеры к более сложной автоматной модели – линейным автоматам Мили, или ЛПС Мили.

Для описания функционирования таких автоматов по шкале времени от “настоящего” в “прошлое” рассмотрим их автоматные функции.

Если обычная ЛПС Мили описывается функциями (2) и (3), тогда для обратной ЛПС Мили используются функции переходов и выходов:

$$S(t) = A_{inv} \times (S(t+1) + BU(t)), \quad GF(2), \qquad (11)$$

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2). \qquad (12)$$

Для упрощения вычислений удобнее использовать несколько другую функцию выходов:

$$Y(t) = C \times S(t+1) + D \times U(t), \quad GF(2). \qquad (13)$$

Восстановление самосинхронизирующего скремблера, как и аддитивного, происходит за два этапа:

– нахождение конечного состояния $S(n)$ ЛПС;

– восстановление в обратном порядке состояний ЛПС и последовательности I.

Для нахождение состояния $S(n)$ необходимо решить систему уравнений, в которой входит также r-битовое слово $u(n), \dots, u(n-r+1)$, равное последним r битам последовательности I:

$$\begin{cases} y(n-r+1) = C \times S(n-r+1) + u(n-r+1); \\ y(n-r+2) = C \times S(n-r+2) + u(n-r+2); \\ \dots \\ y(n) = C \times S(n) + u(n). \end{cases}$$

Как и для аддитивного скремблера, здесь также предполагается, что должны быть известны последние r бит исходной информации (в данном случае последовательности I) и аналогичные им биты скремблированной информации (последовательности Z) (рис. 3).

На втором этапе необходимо поочередно вычислять предыдущее состояние $S(t)$ ЛПС Мили по его текущему состоянию $S(t+1)$, начиная с $S(n)$.

С этой целью определим слово $U(t)$ из (13):

$$U(t) = C \times S(t+1) + Y(t), \quad GF(2)$$

и подставим его в (11):

$$S(t) = A_{inv}(((S(t+1) + B(Y(t) + CS(t+1))), \quad GF(2).$$

(1×1)-матрица D для одновходовой ЛПС равна 1, поэтому ее можно не указывать.

В итоге с линейной сложностью будут восстановлены в обратном порядке все состояния ЛПС и вся последовательность I. Все действия одинаковы для обеих типов ЛПС: Фибоначчи и Галуа. Как и

для аддитивных скремблеров, в общем случае известные r -битовые фрагменты могут начинаться с произвольного i -го разряда неизвестных последовательностей I и Z – тогда также можно выполнять вычисления как вперед, так и назад во времени.

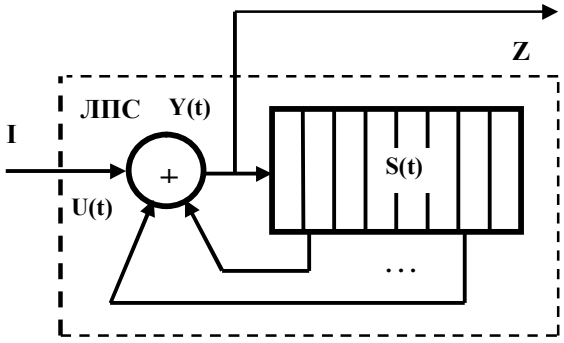

Рис. 3. Самосинхронизирующийся скремблер на основе ЛПС типа Фибоначчи

Отметим, что в [14] показан способ генерации обратных элементов в полях Галуа, который эквивалентен использованию обратной временной модели. Но этот способ применим только для линейных автоматов Мура.

Заключение

РСЛОС являются наиболее популярным схемотехническим узлом в задачах скремблирования и поточного шифрования. И хотя уже много десятилетий ведется теоретическое исследование их свойств, по-прежнему появляются новые их возможности.

Давно известно, что источники новых знаний часто появляются на стыках разных отраслей науки, особенно, близких по сути. Для криптографии такой близкой отраслью является помехоустойчивое кодирование. Имеются многочисленные примеры применения алгебраической теории кодирования для различных шифросистем [15]. В настоящей работе предлагается еще один вариант такого плодотворного взаимодействия. Если применить в задачах шифрования теорию ЛПС и автоматные представления циклических кодов, тогда можно получить много новых перспективных направлений для дальнейших исследований. Одним из них является использование в криптографии темпоральных (временных) моделей.

Список литературы

1. Шевкопляс Б.В. Скремблирование передаваемых данных / Б.В. Шевкопляс // Схемотехника. – 2004. – № 12. – С. 24-27.

2. Стасев Ю.В. Исследование методов криптоанализа поточных шифров [Электронный ресурс] / Ю.В. Стасев, А.В. Потий, Ю.А. Избенко. – Режим доступа к ресурсу: http://www.nrjetix.com/fileadmin/doc/publications/articles/ stasev_potiy_izbenko_ru.pdf.

3. Cluzeau M. Reconstruction of a Linear Scrambler / M. Cluzeau // IEEE Trans. on Computers. – Sep., 2007. – Vol. 56. – No. 9. – P. 1283-1291.

4. Liu X.-B. Reconstructing a Linear Scrambler With Improved Detection Capability and in the Presence of Noise / X.-B. Liu, S. N. Koh, X.-W. Wu, C.-C. Chui // IEEE Trans. on Inf. For. and Sec. – Feb., 2012. – Vol. 7, no. 1. – P. 208-218.

5. Блейхут Р. Теория и практика кодов, исправляющих ошибки [Текст] / Р. Блейхут. – М.: Мир, 1986. – 576 с.

6. Wu X-W. Primitive Polynomials for Robust Scramblers and Stream Ciphers Against Reverse Engineering [Text] / X-W. Wu, S. N. Koh, C.-C. Chui // Proceedings of the ISIT 2010, Austin, Texas, U.S.A., June, 13-18, 2010. – P. 2473-2477.

7. Гилл А. Линейные последовательностные машины [Текст] / А. Гилл; пер. с англ. – М.: Наука, 1974. – 288 с.

8. Семеренко В.П. Теорія циклічних кодів на основі автоматних моделей: монографія [Текст] / В.П. Семеренко. – Вінниця: ВНТУ, 2015. – 444 с.

9. Семеренко В.П. Высокопроизводительные алгоритмы для исправления независимых ошибок в циклических кодах / В.П. Семеренко // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2010. – Вип. 3(84). – С. 80-89.

10. Хокинг С. Краткая история времени: от Большого взрыва до черных дыр. – СПб.: Амфора, 2008. – 231 с.

11. Пригожин И. Время, хаос, квант / И. Пригожин, И. Стенгерс. – М.: Издат. группа Прогресс, 1994. – 272 с.

12. Семеренко В.П. Темпоральные модели параллельных вычислений [Текст] / В.П. Семеренко // Austrian Journal of Technical and Natural Sciences. – 2014. – Vol. 1. – P. 13-25.

13. Семеренко В.П. Параллельное декодирование укороченных циклических кодов [Текст] / В.П. Семеренко // Оптико-электронные информационно-энергетические технологии. – 2012. – № 1. – С. 30-41.

14. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях / О.С. Когновицкий. – СПб.: Линк, 2009. – 411 с.

15. Евсеев С.П. Криптографическое преобразование информации в кодовых криптосистемах на эллиптических кодах для каналов с автоматическим переспросом [Текст] / С.П. Евсеев // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2007. – Вип. 8(66). – С. 29-32.

Поступила в редколлегию 18.02.2016

Рецензент: д-р техн. наук, проф. А.А. Борисенко, Сумский государственный университет, Сумы.

РЕКОНСТРУКЦІЯ ЛІНІЙНИХ СКРЕМБЛЕРІВ НА ОСНОВІ АВТОМАТНИХ МОДЕЛЕЙ

В.П. Семеренко

Пропонується теорія лінійних послідовнісних машин (ЛПС) для представлення скремблерів і потокових шифрів, які використовують регістри зсуву. Розглянута модель функціонування адитивного і самосинхронізуючого скремблерів на основі математичного представлення симетрії часу. Показано спосіб відновлення з лінійною складністю в оберненому порядку невідомої псевдовипадкової послідовності по її відомому r -бітовому фрагменту за допомогою r -вимірної ЛПС.

Ключові слова: *скремблери, криптографія, потокове шифрування, лінійні послідовнісні схеми, час, обернений автомат.*

RECONSTRUCTION OF LINEAR SCRAMBLERS BASED ON AUTOMATON MODELS

V.P. Semerenko

The theory of linear finite-state machines (LFSM) for presentation of a scrambler and stream cipher which using the shifting register is suggested. The model of operation of additive and self-synchronized scramblers based on the mathematical representation of time symmetry is considered. The method of reconstruction of the unknown pseudo-random sequence in the reverse order with the linear complexity by using its known r-bit fragment with the help of r-bit LFSM is offered.

Keywords: *scrambler, cryptography, stream encryption, linear finite-state machine, time, reversible automaton.*