Рудницкий Владимир Николаевич, доктор технических наук, профессор, заведующий кафедрой системного программирования, Черкасский государственный технологический университет.
Email: rvn_2008@ukr.net

Рудницький Володимир Миколайович, доктор технічних наук, професор, завідувач кафедри системного програмування, Черкаський державний технологічний університет.

Rudnitskiy Volodymyr, Professor, Doctor of Science in Eng., Head of Academic Department of System Programming, Cherkassy State Technological University.

Узун Илья Афанасьевич, магистр по прикладной математике, аспирант кафедры информатики и управления защитой информационных систем, Одесский национальный политехнический университет.
Email: uzun.illya@gmail.com

Узун Ілля Афанасійович, магістр з прикладної математики, аспірант кафедри інформатики та управління захистом інформаційних систем, Одеський національний політехнічний університет.

Uzun Illya, Master, postgraduate of Academic Department of Informatics and Management of Information Systems Security, Odessa National Polytechnic University.

УДК 511.512

КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ ОБОБЩЕННЫХ МАТРИЦ ГАЛУА И ФИБОНАЧЧИ

Александр Белецкий

Формирование псевдослучайных последовательностей двоичных чисел составляет актуальную проблему, решаемую в криптографии. Наиболее распространенный метод генерации ПСП основан на линейных регистрах сдвига максимального порядка с линейными обратными связями, однозначно описываемых классическими матрицами Галуа и Фибоначчи. В работе рассмотрены вопросы синтеза обобщенных примитивных матриц Галуа и Фибоначчи (а также их сопряженных вариантов) произвольного порядка n над простым полем Галуа характеристики p. Синтез матриц базируется на использовании неприводимых полиномов fn степени n характеристики p и примитивных элементов расширенного поля Галуа, порождаемого полиномом fn. Обсуждается перспектива применения таких матриц при построении обобщенных генераторов псевдослучайных последовательностей p-ичных чисел и в других областях. Разработаны операторы преобразования любой из обобщенных матриц во все остальные. Предложено стилизованное представление обратных связей в ЛРС-генераторах ПСП.

Ключевые слова: *неприводимые полиномы, примитивные матрицы, примитивные элементы поля Галуа.*

Введение. В теории и практике криптографической защиты информации одной из ключевых проблем является проблема формирования псевдослучайных последовательностей (ПСП) максимальной длины (m-последовательностей) с приемлемыми статистическими характеристиками. Генераторы ПСП реализуют, как правило, на основе линейных регистров сдвига (ЛРС) максимального периода с линейными обратными связями [1]. Для того чтобы ЛРС был регистром максимального периода, соответствующий полином обратной связи должен быть примитивным полиномом (ПрП) $\bmod 2$. По аналогии с полями Галуа [2] введем понятие «характеристика неприводимого полинома», предполагая, что неприводимый полином (НП) степени n, обозначим его векторную форму $f_n = \{\alpha_i\}$, $i = \overline{0,n}$, является полиномом характеристики p, если коэффициенты полинома $\alpha_i \in GF(p)$, причем p – простое число.

В данной статье мы расширим понятие ЛРС, полагая, что каждый его разряд (ячейка памяти) может находиться в одном из состояний $s \in GF(p)$. Назовем такие регистры «обобщенными ЛРС». Обратные связи в обобщенных регистрах максимального периода, определяемого значением $p^n - 1$, формируются неприводимыми полиномами характеристики $p \geq 2$.

Основная задача данного исследования состоит в разработке алгоритмов построения обобщенных матриц Галуа и Фибоначчи $n-$го порядка над полем $GF(p)$, $p \geq 2$, однозначно определяющих как структуру соответствующих обобщенных $n-$разрядных ЛРС максимального периода, так и формируемых ими (регистрами)

псевдослучайных последовательностей чисел максимальной длины p^n-1.

Основная часть. Пусть $A=(a_{i,j})-$ невырожденная матрица порядка $n>1$ над полем целых чисел таких, что $a_{i,j}\in GF(p)$ для всех $i,j=\overline{1,n}$, и E - единичная матрица того же порядка, что и A. Последовательность степеней матрицы A образует циклическую группу порядка e. Матрицу A будем называть «примитивной», если наименьшее натуральное e, при котором $A^e=E$, удовлетворяет соотношению

$$e=p^n-1. \qquad (1)$$

Термин «примитивная матрица» подобен термину «примитивный элемент» расширенного поля $GF(p^n)$. Простейшим примером двоичных примитивных матриц являются матрицы, адекватно отображающие процесс формирования ПСП посредством ЛРС (генераторов) по схемам Галуа и Фибоначчи [3]. Матрицы, моделирующие упомянутые генераторы ПСП, будем именовать матрицами Галуа G и Фибоначчи F соответственно.

Матрица Фибоначчи является частным случаем матрицы Фробениуса [4] и имеет вид:

$$F=\begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & \alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & \alpha_{n-1} \end{bmatrix}, \qquad (2)$$

где α_i – коэффициенты ПрП f_n.

Транспонируя F относительно вспомогательной диагонали, приходим к матрице Галуа.

Следовательно, матрицы G и F связаны оператором «правостороннего транспонирования» $\perp$, т. е.

$$G\overset{\perp}{\longleftrightarrow}F \qquad (3)$$

На основании соотношений (2) и (3) приходим к матрице

$$G=\begin{bmatrix} \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_1 & \alpha_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}, \qquad (4)$$

Матрицы (3) и (4) будем именовать «базовыми матрицами» генераторов ПСП. Кроме рассмотренных матриц Галуа G и Фибоначчи F каждой из них могут быть поставлены в соответствие так называемые «сопряженные матрицы» G^* и F^*, которые вводятся [5] преобразованиями:

$$\begin{aligned} G^*&=1\cdot G\cdot 1; \quad G=1\cdot G^*\cdot 1; \\ F^*&=1\cdot F\cdot 1; \quad F=1\cdot F^*\cdot 1, \end{aligned} \qquad (5)$$

где 1 – условное обозначение оператора инверсной перестановки (ИП), представляющего собой квадратную инволютивную матрицу n-го порядка, на вспомогательной диагонали которой стоят единицы, а в остальных элементах нули.

Общая форма сопряженных матриц Галуа и Фибоначчи представлена соотношениями (6) и (7) соответственно

$$G^*=\begin{bmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & 1 & \cdots \\ 0 & 0 & \cdots & 0 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} & \alpha_{n-1} \end{bmatrix}, \qquad (6)$$

$$F^*=\begin{bmatrix} \alpha_{n-1} & 1 & \cdots & 0 & 0 \\ \alpha_{n-2} & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & 1 & 0 \\ \alpha_1 & 0 & \cdots & 0 & 1 \\ \alpha_0 & 0 & \cdots & 0 & 0 \end{bmatrix}. \qquad (7)$$

Из сопоставления базовых матриц G и F, а также их сопряженных вариантов G^* и F^*, легко могут быть определены операторы преобразования одной из известных матриц в любую другую матрицу. Полный набор операторов преобразования представлен в табл. 1. В этой таблице обозначены: $1\circ 1$ – оператор «сопряжения» (5), а $1\perp 1$ – составной оператор, включающий операторы «сопряжения» и правостороннего транспонирования.

Таблица 1

Операторы преобразование матриц

	G	F	G^*	F^*
G	—	$\perp$	$1\circ 1$	$1\perp 1$
F	$\perp$	—	$1\perp 1$	$1\circ 1$
G^*	$1\circ 1$	$1\perp 1$	—	$\perp$
F^*	$1\perp 1$	$1\circ 1$	$\perp$	—

Базовые матрицы (4) и (3) и их сопряженные варианты (6) и (7), являются классическими примитивными матрицами Галуа и Фибоначчи соответственно. Такие матрицы отвечают ЛРС максимального порядка, для формирования обратных связей в которых используются исключительно ПрП характеристики 2. Ниже на рис. 1-4 показаны структурные схемы всех четырех типов двоичных восьмиразрядных ЛРС. Двоичные связи в этих генераторах ПСП формируются ПрП $f_8=101001101$.

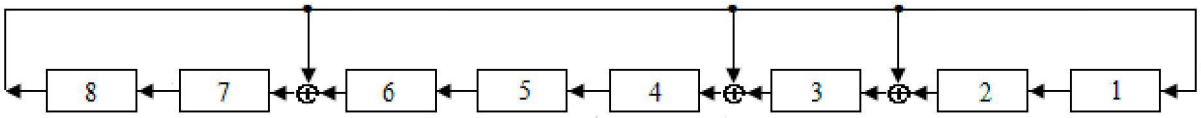

Рис. 1. Структурная схема генератора ПСП Галуа

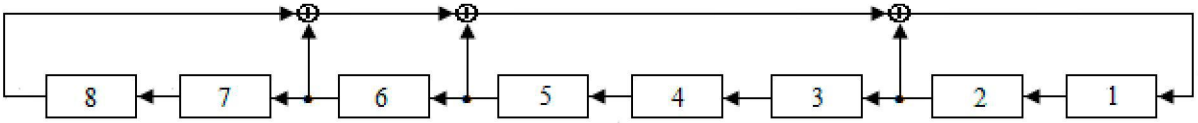

Рис. 2. Структурная схема генератора ПСП Фибоначчи

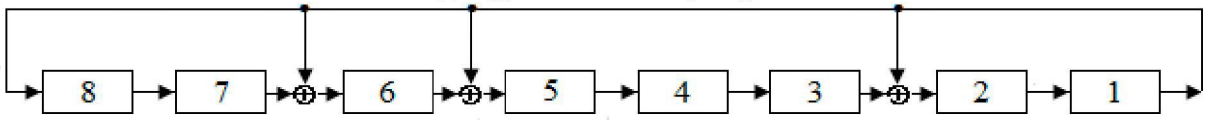

Рис. 3. Структурная схема сопряженного генератора ПСП Галуа

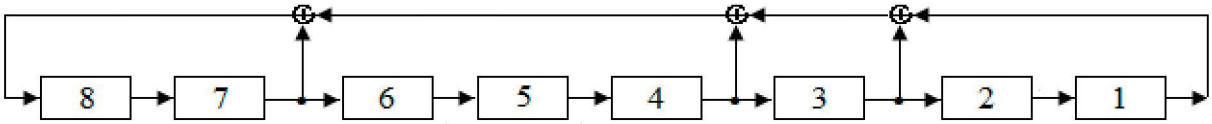

Рис. 4. Структурная схема сопряженного генератора ПСП Фибоначчи

Обратим внимание на то, что если в базовых генераторах ПСП (рис. 1, 2) схемы обратных связей (ОС) «закручены» по часовой стрелке, то в сопряженных (рис. 3, 4) – против часовой стрелки. Общие правила преобразования схем линейных ОС известного генератора к схемам обратных связей любого их оставшихся генераторов сведены в табл. 2.

В табл. 2 схема обратных связей, обозначенная символом $1\circ$, претерпевает вращение относительно горизонтальной оси, символом $\circ 1$ – относительно вертикальной оси, тогда как символ (оператор) $1\circ 1$ означает вращение схемы ОС относительно обеих центральных осей симметрии. Цифра 1 (ИМ), расположенная слева оператора ОС, символизирует перестановку «строк», а справа – «столбцов» схемы ОС.

Смысл термина «схемы обратных связей» ЛРС генераторов ПСП (на примере генераторов, структурные схемы которых представлены на рис. 1-4) можно пояснить, обратившись к их стилизованному отображению, показанному на рис. 5.

Таблица 2

Операторы преобразования ОС

	G	F	G^*	F^*
G	—	$1\circ 1$	$\circ 1$	$1\circ$
F	$1\circ 1$	—	$1\circ$	$\circ 1$
G^*	$\circ 1$	$1\circ$	—	$1\circ 1$
F^*	$1\circ$	$\circ 1$	$1\circ 1$	—

Суть алгоритма синтеза обобщенных примитивных матриц Галуа, элементы которых $\alpha_{i,j}$, $i,j=\overline{1,n}$, принадлежат расширенному полю $GF(p^n)$, заключается в следующем [6].

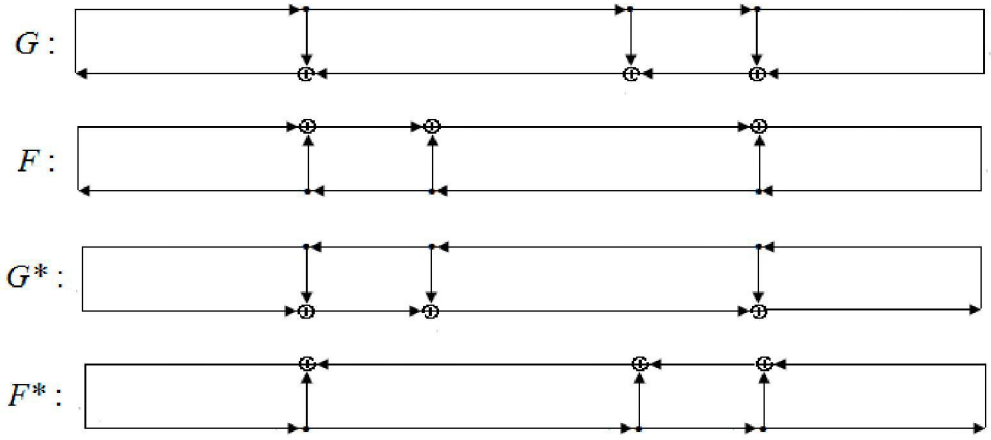

Рис. 5. Стилизованное представление обратных связей в ЛРС-генераторах ПСП

Пусть ω – образующий элемент матрицы, в качестве которого может быть выбран любой примитивный элемент поля $GF(p^n)$, порождаемого НП f_n. ОЭ ω записывается в нижней (первой) строке матрицы G. Элементы строки, расположенные левее ω, заполняются нулями. Последующие строки матрицы G (по направлению снизу вверх) образуются круговой прокруткой по часовой стрелке предыдущих строк матрицы. Если при этом левый элемент прокручиваемой строки равен 1, то выполняется обычный сдвиг строки на один разряд влево, а в правый освободившийся элемент строки записывается 0. При этом разрядность строки становится на единицу больше порядка матрицы. Векторы, отвечающие таким строкам, приводятся к остатку по модулю НП f_n и, тем самым, длина строки возвращается к порядку, равному порядку матрицы n.

Пусть $s_k^{(t)}$, $k=\overline{1,n}$, $t=0,1,\ldots$ – состояние k-го разряда (p-ичного D-триггера) ЛРС с обобщенными линейными обратными связями в дискретный момент времени t, причем $s_1^{(0)}=1$, $s_k^{(0)}=0$, $k=\overline{2,n}$. Кроме того, обозначим $h_{i,j}$ элемент i-й строки и j-го столбца, $i,j=\overline{1,n}$, любой из матриц G, F, G^* или F^*. Строки матриц, как отмечено выше, нумеруются снизу вверх, а столбцы – справа налево.

Состояние k-го разряда ЛРС $s_k^{(t+1)}$ в момент времени $t+1$ совпадает с функцией возбуждения этого разряда $\nu_k^{(t)}$ в момент времени t и определяется соотношением:

$$s_k^{(t+1)}=\nu_k^{(t)}=\bigoplus_{i=1}^{n} h_{i,k}\cdot s_k^{(t)}. \qquad (8)$$

Пусть, для примера, $n=4$, НП $f_4=11111$ и ОЭ $\omega=111$. Примитивные двоичные матрицы Галуа G и Фибоначчи F, а также их сопряженные варианты G^* и F^*, имеют вид:

$$G=\begin{pmatrix}0&1&1&0\\0&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix};\quad F=\begin{pmatrix}1&0&1&0\\1&1&1&1\\1&1&0&1\\0&1&0&0\end{pmatrix};\quad G^*=\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\\0&1&1&0\end{pmatrix};\quad F^*=\begin{pmatrix}0&0&1&0\\1&0&1&1\\1&1&1&1\\0&1&0&1\end{pmatrix}. \qquad (9)$$

Обобщенная структурная схема базового четырехразрядного генератора ПСП Галуа и совпадающая с ней схема генератора Фибоначчи, построенная на основании соотношения (8), представлена на рис. 6. Вертикально расположенные регистры генераторов, отмеченные сверху символом $\otimes$, в которые вводятся столбцы матриц преобразования G или F, реализуют операцию поразрядного умножения, а регистры, отмеченные символом $\oplus$ – операцию сложения содержимого регистра по модулю 2. Если в регистрах умножения разместить элементы столбцов матрицы G, то получим генератор ПСП по схеме Галуа. В том случае, когда в те же регистры вводятся элементы столбцов матрицы F, то образуется генератор ПСП по схеме Фибоначчи.

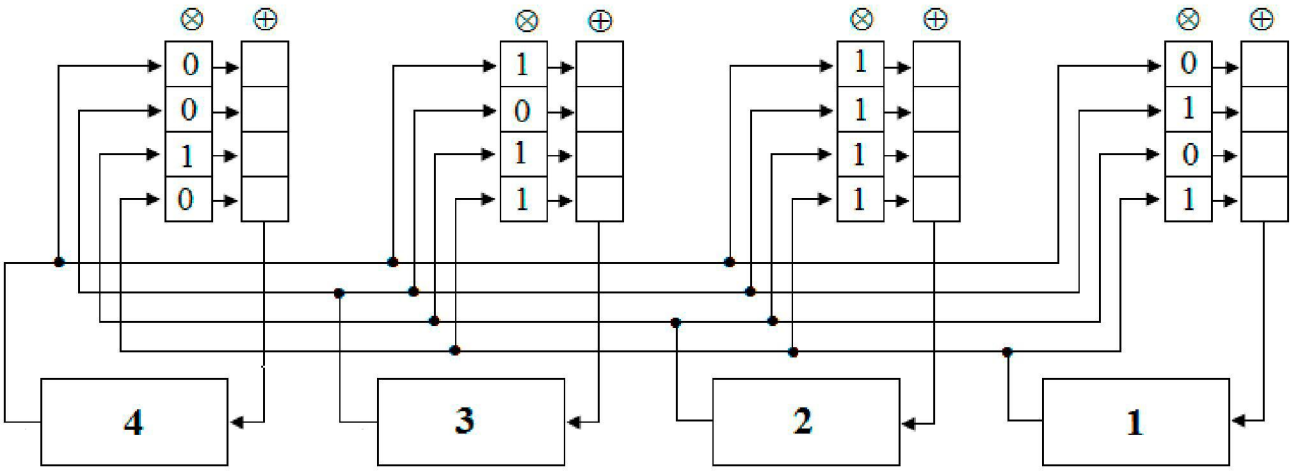

Рис. 6. Схема базовых генераторов ПСП G / F

Структурная схема сопряженных генераторов ПСП Галуа и Фибоначчи показана на рис. 7.

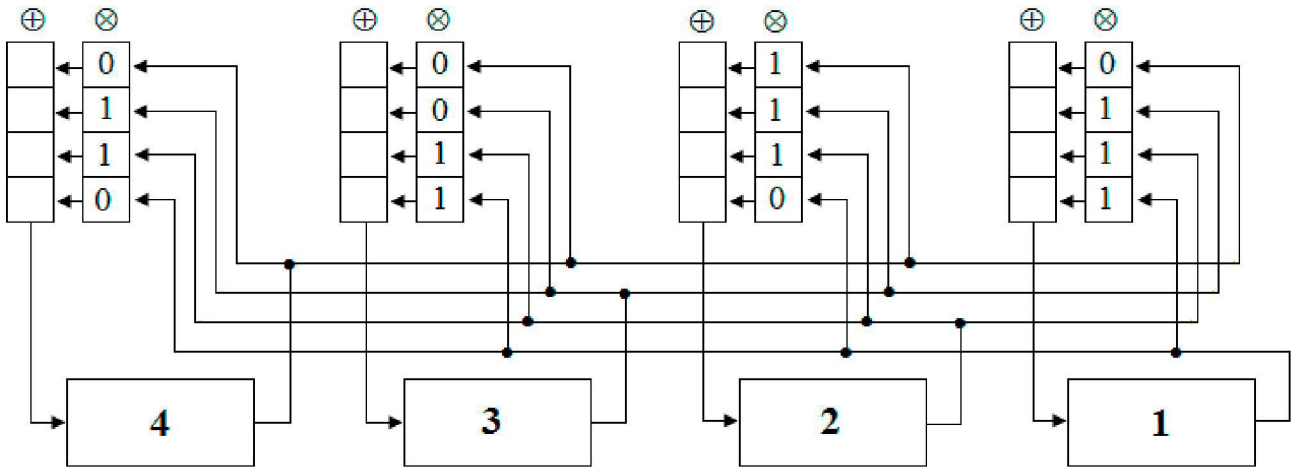

Рис. 7. Схема сопряженных генераторов ПСП G^* / F^*

В регистры перемножения на рис. 6 введены столбцы матрицы G системы (9), а на рис. 7 – столбцы матрицы F^*.

Предлагаемый алгоритм с равным успехом может быть применен для синтеза примитивных матриц, элементы которых $a_{i,j}$ принадлежат полю $GF(p)$ произвольной характеристики p. В качестве примера соотношением (10) показаны результаты синтеза матриц с параметрами: $p=3$, $n=4$, $\mathrm{f}_4=12101$.

$$G=\begin{pmatrix}1&1&1&2\\1&0&2&1\\2&2&2&2\\1&1&0&2\end{pmatrix};\quad F=\begin{pmatrix}2&2&1&2\\0&2&2&1\\1&2&0&1\\1&2&1&1\end{pmatrix};\quad G^*=\begin{pmatrix}2&0&1&1\\2&2&2&2\\1&2&0&1\\2&1&1&1\end{pmatrix};\quad F^*=\begin{pmatrix}1&1&2&1\\1&0&2&1\\1&2&2&0\\2&1&2&2\end{pmatrix}. \qquad (10)$$

Заключение. Основным результатом данного исследования является разработка алгоритмов синтеза обобщенных базовых и сопряженных матриц Галуа и Фибоначчи, элементы которых принадлежат простому полю $GF(p)$ характеристики $p \geq 2$. Такие матрицы обладают рядом замечательных свойств, а именно, примитивностью и коммутативностью, что дало возможность построить на их основе обобщенные линейные регистры сдвига максимального периода. Структурно-логические схемы обобщенных линейных регистров сдвига оказались однородными и инвариантными как к порядкам регистров, так и к характеристикам поля Галуа.

ЛИТЕРАТУРА

[1]. Поточные шифры. Результаты зарубежной открытой криптологии / [Электронный ресурс]. – Режим доступа: http//www.ssl.stu.neva.ru /psw/ crypto.html.

[2]. Лидл Р. Конечные поля /Р. Лидл, Г. Нидер-Райтер. Т. 1. – М.: Мир, 1988. – 432 с.

[3]. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. / М.А. Иванов, И.В. Чугунков – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

[4]. Гантмахер Ф. Р. Теория матриц. / Ф.Р. Гантмахер — М.: Физматлит, 2004. — 560 с.

[5]. Белецкий А.Я. Преобразования Грея. Монография в 2-х томах. / А.Я. Белецкий, А.А. Белецкий, Е.А. Белецкий. Т. 1. Основы теории – К.: Кн. Изд-во НАУ, 2007. – 412 с.

[6]. Белецкий А.Я. Синтез примитивных матриц в конечных полях Галуа и их применение. / А.Я. Белецкий, А.А. Белецкий // Информационные технологии в образовании. – Херсон: ХГУ, 2012. – С. 23–43.

[7]. Белецкий А.Я. Примитивные матрицы над простыми полями Галуа. /А.Я. Белецкий // Системи обробки інформації. – Х. ХУПС. – 2012, № 3. – С. 218-219.

REFERENCES

[1]. Stream ciphers. The results of the open foreign cryptology / [electronic resource]. - Mode of access: http//www.ssl.stu.neva.ru /psw/ crypto.html.

[2]. R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge university press, 1994, 416 p.