Дмитриев Д.С.
Система доступа к персональным данным предприятия на основе линейной рекуррентной последовательности // Вестник Самарского государственного университета. Серия «Экономика и управление». 2015. № 9/1 (131). С. 258–263

УДК 330.42

Д.С. Дмитриев*

СИСТЕМА ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ ПРЕДПРИЯТИЯ НА ОСНОВЕ ЛИНЕЙНОЙ РЕКУРРЕНТНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

В статье определены основные аспекты создания подсистемы доступа к персональным данным предприятия на основе математического аппарата линейных рекуррентных последовательностей, заданных над конечными примарными кольцами. Подсистема учитывает аспекты индекса появления элементов на цикле линейной рекуррентной последовательности.

Ключевые слова: линейные рекуррентные последовательности, регистр с линейной обратной связью, персональные данные организации, e-learning.

В настоящее время проблема защиты информации касается многих организаций, которые сталкиваются с системами обработки персональных данных, схемами генерации электронно-цифровых подписей, получением сертификатов. Одними из наиболее востребованных систем шифрования и кодирования данных являются приложения на основе псевдослучайных линейных рекуррентных последовательностей (ЛРП): развивается теория генераторов псевдослучайных последовательностей, изучаются статистические и частотные свойства ЛРП над конечными полями, конечными кольцами, в частности над кольцами вычетов. Однако математический аппарат, связанный с теорией и свойствами ЛРП, недостаточно адаптирован с практической точки зрения в контексте реализации прикладного программного обеспечения. В статье рассмотрены практические основы системы доступа к персональным данным предприятия на основе линейных рекуррентных последовательностей с учетом конструкции разграничения доступа на базе регистра с линейной обратной связью (РСЛОС). Математический регистр создается на основе ЛРП над конечным кольцом вида Z_{p^n}, где p, n – натуральные числа.

1. Индекс появления элемента последовательности над конечным кольцом.

Теория ЛРП над конечными полями имеет достаточно завершенный характер [1]. При переходе к случаю колец, которые не являются полями, теория претерпевает изменения даже в таком хорошо изученном случае, как примарные кольца вычетов. Одной из значимых задач описания ЛРП является исследование частотных характеристик последовательностей для создания более эффективно работающей системы шифрования [2]. Для вычисления параметров прикладных систем, основанных на ЛРП, важно знать распределение элементов в линейных рекуррентах. Но на первый план выходит вопрос, все ли элементы кольца встречаются в ЛРП. В связи с этим представляет интерес исследование индексов вхождений элементов в ЛРП. В частности, полезно получить условия, при которых каждый элемент кольца появляется в ЛРП.

На основе [3–5] получены результаты индексов вхождений элементов для реверсивного многочлена Галуа над кольцом Z_8.

Дмитриев Денис Сергеевич (denisdmitriev000@gmail.com), кафедра математики и бизнес-информатики, Самарский государственный университет, 443011, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.

Пусть имеем некоторую ЛРП u, заданную над примарным кольцом Z_8 с характеристическим многочленом $F(x)$ и редукцией $F_1(x)$. Обозначим через $I_u(z)$ величину индекса вхождения элемента z в последовательность u [5]. Условие конечности $I_u(z)$ с общего случая переносится на случай кольца Z_8.

Кольцо вычетов $Z_8 = Z_{2^3}$, т. е. $p = 2, n = 3$.

Тогда

$$T(F_1) \geq (8-1) * 2^{\frac{m}{2}+3-1} \geq 7 * 2^{\frac{m}{2}+2}. \quad (1)$$

В итоге имеем $T(F_1) \geq 28 * 2^{\frac{m}{2}}$.

Максимальный период редукции $T_{max} = p^m - 1$ (по определению многочлена максимального периода над конечным полем), где m – степень многочлена $F(x)$ [5; 6]. Таким образом, для случая Z_8 имеем $2^m - 1 \geq 28 * 2^{\frac{m}{2}}$. Производя замену $t = 2^{\frac{m}{2}}$ и решая квадратичное неравенство, получаем, что для редукций максимального периода $t \geq 29$. Таким образом, для многочленов максимального периода условие конечности индекса вхождения элементов в ЛРП имеет вид $m \geq 10$

Пусть ЛРП u имеет над Z_8 характеристический многочлен вида $F(x) = x^m - x - 1$. Кольцо Z_8 состоит из классов вычетов $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Заметим, что для каждой ЛРП u из $L(F)^*$ последовательность $-u$ также принадлежит множеству $L(F)^*$, аналогично $3u$ и $5u$ принадлежат $L(F)^*$. Исходя из этого получаем, что

$$I_F(1) = I_F(3) = I_F(5) = I_F(7). \quad (2)$$

Именно поэтому без ограничения общности будем искать $I_F(7)$. Обозначим через l минимальное целое неотрицательное число i такое, что $u(i) \in \{1, 3, 5, 7\}$. По выбору ЛРП u выполнено неравенство $l \leq m - 1$. Без ограничения общности будем считать, что $u(l) = 1$.

Произведем поиск $I_F(7)$ для ЛРП u с характеристическим многочленом $F(x) = x^3 - x - 1 \in Z_8[x]$. По теореме о вычислении периода многочлена над кольцом $T(F(x)) = 28$. Закон рекурсии для данного многочлена выглядит следующим образом:

$$u_{l+3} = u_{l+1} + u_l. \quad (3)$$

Тогда элемент $u_l = 7$ на цикле ЛРП можно получить в следующих случаях, обозначенных в таблице.

Таблица

Возможности получения элемента $u(l) = 7$ на цикле ЛРП u

$u(l)$	$u(l-3), u(l-2)$
7	**3, 4**
7	**4, 3**
7	**5, 2**
7	**2, 5**
7	**6, 1**
7	**1, 6**

Степень многочлена равна трем, соответственно, начальный вектор u должен состоять из трех элементов, т. е. $u\{0,2\} = (u(0), u(1), u(2))$. Тогда, продолжая цепочку, рассматривая варианты для получения элементов $u(l-3), u(l-2)$, исключая из рассмотрения случаи, где в качестве одного из элементов последовательности встречается 7, получим все возможности получения элемента $u(l) = 7$ на цикле ЛРП u при начальном векторе с тремя координатами. Для случаев, когда среди элементов начального вектора есть хотя бы один необратимый элемент, получим, что $u(l) = 7$ встречается при вычислении каждой такой ЛРП. Вычисляя $I_u(7)$ для каждой полученной ЛРП, получим, что $I_F(7) = 27$.

Перейдем к получению оценки над кольцом $R = Z_8$. Обозначим в качестве кольца $S = Z_2 = F_2$ – поле. Зададим произвольное отображение $\sigma: R \to S$, действующее по следующему правилу:

$$\forall\, z \in S: \sigma(z) = 1 \;\boldsymbol{и}\; \sigma(x) \neq 0, x \neq z \tag{4}$$

Обозначим через $\Gamma(Z_8)$ множество всех элементов x кольца R, таких, что $x^2 - x = 0$, т.е. $x^2 = x$. Таким образом, $\Gamma(Z_8) = \{-0, -1\}$. Найдется единственный многочлен $H(x_0, x_1)$ над F_2, имеющий степень переменной не выше 2, такой что $\sigma(a) = H\,(0,1,2,3,4,5,6,7), \forall\, a \in R$. Таким образом, значение k для Z_8 вычисляется следующим образом: $k = k_0 + k_{12} + k_{22}^2$, что соответствует разложению $\forall\, a \in Z_8$.

Каждый элемент $a \in Z_8$ может быть выражен так: $a = a_0 + 2a_1 + 2^2 a_2$, где $a_i \in \Gamma(Z_8)$, для всех $a_i \in \Gamma(Z_8)$, $i \in \{0,2\}$. Искомый элемент $x = 7$ при таком разложении имеет вид: $7 = 1 + 1 * 2 + 1 * 2^2$.

Получаем, что

$$\Sigma(a) = H(a_0, a_1, a_2) = (1 - (a_0 - 1^1)(1 - (a_1 - 1^1))(1 - (a_2 - 1^1))). \tag{5}$$

Раскрывая скобки, видим, что $\Sigma(a) = H(a_0, a_1, a_2) = a_0 a_1 a_2$. Все мономы, входящие в многочлен H, имеют первую степень. Отсюда, рассмотренный параметр k будет равен 7.

В случае с кольцом Z_8 $p = 2$, подсчет оценки $I_u(7)$ будем выполнять следующим образом [5; 7]:

$$I_u(7) = \sum_{A=0}^{3} (A+1) \sum_{N=b(A+1)+1}^{b(A)} \left\{ {m \atop N} \right\}_2. \tag{6}$$

Остается вычислить значения $b(A)$: $b(A=1) = 7 - 2*1 + 1 = 6$. Аналогично вычисляя, получаем $b(A=2) = 3, b(A=3) = 3, b(A=4) = 0$. Подставим полученные значения в формулу и вычислим оценку величины $I_u(7)$:

$$\begin{aligned} I_u(7) < 1\left(\binom{m}{8} + \binom{m}{7}\right) + 2\left(\binom{m}{6} + \binom{m}{5}\right) + 3\left(\binom{m}{4} + \binom{m}{3}\right) \\ + 4\left(\binom{m}{3} + \binom{m}{2} + \binom{m}{1}\right). \end{aligned} \tag{7}$$

Вычисляя биномиальные коэффициенты, получаем:

$$I_u(7) < \frac{(m-1)(m-2)(m-3)(m-4)(m-5)(m-6)(m-7)}{8!}. \tag{8}$$

В итоге

$$I_u(7) < \frac{\mathrm{m}^7 - 4\mathrm{m}^6 + 2\mathrm{m}^5 + \mathrm{m}^3 - 4\mathrm{m}^2 + 4\mathrm{m}}{8!}. \tag{9}$$

2. Практическое применение на основе подсистемы доступа к персональным данным организации.

В современных реалиях работа с персональными данными в любых организациях (коммерческих, государственных и т. п.) выходит на одно из лидирующих мест в контексте соответствия законодательству Российской Федерации, а также корректной обработки. Естественным является ориентация на упрощение доступности, удешевление стоимости систем, повышение их эффективности. Ориентация на сокращение времени, затрачиваемого на работу с персональными данными и получение доступа к ним, обусловливает необходимость внедрять на предприятиях системы защиты информации, а также производить некоторые доработки таких программных продуктов с учетом индивидуальных требований предприятий (при возможности таковой). Подобная система может применяться также при работе центров дополнительного профессионального образования и быть сконструирована на базе системы электронного обучения (E-learning) [8–10].

```
1  Working in ring Z8
2  Input the beginning values of lfsr. Count of elements:5
3  Input 0 element 1
4  Input 1 element 3
5  Input 2 element 5
6  Input 3 element 2
7  Input 4 element 7
8  Inputting number of connection and coefficients of
9  connection. 1..4 - connection is in lfsr with this
10 coefficient, 0 - there is no connecction by this
11 number in lfsr
12 Is 0 connection in lfsr? 1
13 Is 1 connection in lfsr? 2
14 Is 2 connection in lfsr? 3
15 Is 3 connection in lfsr? 1
16 Is 4 connection in lfsr? 1
17 Character polynom of lfsr:
18 f(x) = 1x^5 - 1x^4 - 1x^3 - 3x^2 - 2x - 1
```

Рис. 1. Вывод информации о заполнении регистра

```
1 135277164214101545264655267241773547770603436354 1
2 022237647645513167756465054110126425122320177310 7
3 730647072310502263360360 55.
```

Рис. 2 Вывод ключа

На самарском предприятии ЗАО «Самарская лука» была разработана логика генерации уникального ключа, открывающего доступ руководителю предприятия к подсистеме персональных данных сотрудников организации. Такая ситуация была взята за основу при создании программного приложения, способного генерировать подобный ключ, который был бы устойчивым к компрометации. На языке программирования Java была реализована системообразующая функция (рис. 1), входными параметрами которой являются известный только руководителю предприятия, выполняющему основную работу по обработке персональных данных, тип регистра с линейной обратной связью (РСЛОС), спроектированной на основе математического аппарата, описанного ранее. Параметры РСЛОС включают в себя

длину регистра, коэффициенты РСЛОС, наличие связей в ячейках, начальное заполнение регистра и кольцо вычетов, над которым производятся математические операции. На основе регистра и указанных связей генерируется ЛРП, которая и является ключом шифрования для криптографического алгоритма, с помощью которого выполняется доступ к подсистеме персональных данных сотрудников.

Для реализации был выбран регистр длины $n = 5$ с начальным заполнением $u\{0,5\} = (1,2,3,2,1)$, заданный в примарном кольце вычетов Z_4.

Приведем конкретный пример вывода, формируемого приложением, для выбранного регистра длины $n = 5$ с указанным начальным заполнением.

Линейная рекуррентная последовательность (сам ключ), выработанная в результате работы функции и находящаяся в текстовом файле (адрес расположения файла указывается в тексте программы), представлена на рис. 2.

Именно эту последовательность и следует подавать на вход руководителю предприятия для доступа к подсистеме персональных данных его сотрудников.

Таким образом, для желающего заполучить несанкционированный доступ к персональным данным встает задача сложности нахождения длины регистра и наличия связей (что эквивалентно задаче нахождения характеристического многочлена ЛРП, генерируемой регистром), а также кольца вычетов, в котором производятся математические вычисления.

Библиографический список

1. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: учебник в 2 т. Т. 2. М.: Гелиос АРВ, 2003. 416 с.

2. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин [и др.]. 3-е изд. М.: Гелиос АРВ, 2005. 480 с.

3. Былков Д.Н., Камловский О.В. Индексы вхождений элементов в линейные рекуррентные последовательности над примарными кольцами вычетов // Проблемы передачи информации. 2008. Т. 44, вып. 2. С. 101–109.

4. Боревич З.И., Шафаревич И.Р. Теория чисел. 3-е изд. М.: Наука, 1985. 504 с.

5. Кузьмин А.С. Распределение элементов на циклах линейных рекуррент над кольцами вычетов // Успехи математических наук в московском математическом обществе. Сообщения московского математического общества. 1992. Т. 47, вып. 6 (288). С. 213–214.

6. Chou W.S., Mullen G.L. Generating linear spans over finite fields // Acta Arith. 1992. V. 61, № 2. P. 183–191.

7. Linear recurring sequences over rings and modules / V.L. Kurakin, A.S. Kuzmin, A.V. Mikhalev [et al.] // J. Math. Sciences. 1995. V. 76, № 6. P. 2793–2915.

8. Андрончев И.К., Соловова Н.В., Дмитриев Д.С. Управление образовательным процессом вуза средствами информационно-коммуникационных технологий // Вестник Самарского государственного университета. 2015. № 8 (119). С. 240–247.

9. Дмитриев Д.С. Системы E-learning: учебное пособие. Самара: Изд-во «Самарский университет», 2014. 32 с.

10. Дмитриев Д.С. Система электронного обучения EFront: учебное пособие. Самара: Изд-во «Самарский университет», 2015. 40 с.

References

1. Glukhov M.M., Elizarov V.P., Nechaev A.A. Algebra: textbook in 2 Vols. Vol. 2. M., Gelios ARV, 2003, 416 p. [in Russian].

2. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Fundamentals of cryptography: 3rd edition. M., Gelios ARV, 2005, 480 p. [in Russian].

3. Bilkov D.N., Kamlovskii O.V. Occurrence Indexes of Elements in Linear Recurrence Sequences over Primary Residue Rings. *Problemy peredachi informatsii* [Problems of Information Transmission], Vol. 44, Issue 2, 2008, pp.101–109 [in Russian].

4. Borevich Z.I., Shafarevich I.R. Number theory: 3rd edition. M., Nauka, 1985, 504 p. [in Russian].

5. Kuzmin A.A. The elements distribution on cycles of residues linear recurrences over rings. *Uspekhi matematicheskikh nauk v moskovskom matematicheskom obshchestve. Soobshcheniia moskovskogo matematicheskogo obshchestva* [Successes of Mathematical Sciences at Moscow Mathematical Society. Communications of Moscow Mathematical Society], Vol. 47, Issue 6(288), 1992, pp. 213–214 [in Russian].

6. Chou W.S., Mullen G.L. Generating linear spans over finite fields. *Acta Arith.* Vol. 61, №2, 1992, pp. 183–191 [in English].

7. Kurakin V.L., Kuzmin A.S., Mikhalev A.V., Nechaev A.A. Linear recurring sequences over rings and modules. *J. Math. Sciences*, Vol. 76, №6, 1995, pp. 2793 – 2915 [in English].

8. Andronchev I.K. Solovova N.V., Dmitriev D.S. Management of the educational process of the university by means of information and communication technologies. *Vestnik Samarskogo gosudarstvennogo universiteta* [Vestnik of Samara State University], 2015, no. 8(119), pp. 240–247 [in Russian].

9. Dmitriev D.S. E-learning systems. Samara, Izd-vo «Samarskii Universitet», 2014, 32 p. [in Russian].

10. Dmitriev D.S. ELearning system EFront. Samara, Izd-vo «Samarskii Universitet», 2015, 40 p. [in Russian].

D.S. Dmitriev*

BUSINESS ORGANIZATION PERSONAL DATA ACCESS SYSTEM BASED ON LINEAR RECCURENCE SEQUENCE

The article defines the main aspects of creation of a subsystem of access to personal data on the basis of the linear recurrence sequences mathematical apparatus of defined over primary order finite rings. Subsystem index takes into account aspects of the elements appearance on linear recurrence sequence cycle.

Key words: linear recurrence sequences, register with linear feedback, personal data of organization, e-learning.

Статья поступила в редакцию 15/VIII/2015.
The article received 15/VIII/2015.

* *Dmitriev Denis Sergeevich* (denisdmitriev000@gmail.com), Department of Mathematics and Business-Informatics, Samara State University, 1, Acad. Pavlov Street, Samara, 443011, Russian Federation.