MOTROL, 2008, 10B, 81-90

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ НА БАЗЕ АППАРАТА КАНОНИЧЕСКИХ РАЗЛОЖЕНИЙ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Igor Atamanyuk

Mykolayiv State Agrarian University, Ukraine

Krylova Street 17, Mykolayiv 54040, Ukraine
e-mail: atamanyuk_igor@mail.ru

Аннотация. В работе получен метод шифрования, который позволяет преобразовать передаваемое сообщение в последовательность независимых значений, что существенно затрудняет задачу вскрытия исходных данных. Алгоритм базируется на каноническом разложении исследуемой случайной последовательности.

Ключевые слова: алгоритм шифрования, линейные стохастические связи.

ВВЕДЕНИЕ

Сегодня в Украине, как и в других странах мира, в процессе предпринимательской деятельности, при создании новых технологий, в результате интеллектуальной работы, возникают насыщенные разнообразными сведениями информационные объекты, которые имеют коммерческую ценность. Это могут быть методики работ, перспективные технические решения, результаты маркетинговых исследований и т.п., нацеленные на достижение предпринимательского успеха.

МЕТОДИКА ИССЛЕДОВАНИЙ

Термин «коммерческая тайна» был введен в правовое обращение Законом Украины «Про підприємства в Україні» от 27.03.1991 г. (потерял силу с 01.01.2004 г.). Под коммерческой тайной предприятия имелись в виду сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, которые не являются государственной тайной, разглашение которых может нанести вред интересам предприятия. С 1 января 2004 года Гражданский кодекс Украины (ГК) определяет такое понятие: «коммерческой тайной является информация, которая является секретной в том понимании, что она в целом или в определенной форме и совокупности ее составляющих является неизвестной и труднодоступной для лиц, которые

обычно имеют дело с видом информации, к которому она принадлежит, в связи с этим имеет коммерческую ценность и является предметом адекватных существующим обстоятельствам мероприятий по сохранению ее секретности, употребленных лицом, которое законно контролирует эту информацию». Статья 505 ГК также определяет, что «коммерческой тайной могут быть сведения технического, организационного, коммерческого, производственного и другого характера, за исключением тех, которые соответственно закону не могут быть отнесены к коммерческой тайне».

Проблемой защиты информации путем ее преобразования математическими методами занимается наука криптология [1-7]. Одним из перспективных направлений криптологии, как известно [8,9], является использование стохастических алгоритмов – методы защиты информации, прямо или косвенно основанные на использовании генераторов псевдослучайных последовательностей. В настоящее время существует два наиболее существенных класса стохастических методов: 1) стохастические алгоритмы, основанные на использовании свойств эллиптических кривых (Elliptic Curves (EC)) [8,10-11]; 2) дихотомические генераторы псевдослучайных последовательностей [8,12].

Методы первого класса являются наиболее математически обоснованными, однако остается открытым вопрос о существовании односторонней функции [6] (зная принцип ее работы и фрагмент выходной последовательности, но, не имея в наличии ключевой информации, криптоаналитик для определения предыдущего выбранного элемента последовательности не может предложить лучшего способа, чем использование жребия). Существуют только функции-кандидаты, претендующие называться односторонними. Примером такого преобразования является дискретное логарифмирование, осуществляемое на группе точек эллиптической кривой. Для точек эллиптической кривой вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах, основанных на задаче факторизации больших чисел (криптосистема RSA) и задаче дискретного логарифма в конечных полях (криптосистема Эль-Гамаля).

Основу алгоритмов второго класса составляют дихотомические операторы, иначе D-операторы. Один из типовых вариантов реализации D-генераторов, преобразующих предыдущий бит B_{i-1} в B_i, представляется самосинхронизирующимся трехпараметрическим оператором $R_H(P_{i-1}, Q_{i-1}, D_{i-1}, H): B_{i-1} \to \{B_i, P_i, Q_i, D_i\}$, с коэффициентом H и косвенным выходом $r_i = Q_{i-1} \oplus P_{i-1}$ или $r_i = Q_{i-1} \oplus D_{i-1}$, составленным из операторов:

$$B_i = B_{i-1} \oplus P_{i-1}, \quad P_i = (2^g \cdot Q_{i-1}) \oplus D_{i-1} \quad (g \geq 2),$$

$$Q_i = B_{i-1} \oplus H, \quad D_i = (2 \cdot (Q_{i-1} \wedge P_{i-1})) \vee 1.$$

Основными достоинствами D-операторов является эффективная программная и аппаратная реализация и возможность построения на их основе всех симметричных криптографических примитивов, однако в силу свойств присущих регулярным D-операторам, младшим битам формируемых на их основе дихотомических последовательностей, присуща существенно выраженная корреляция, которая убывает от младших битов D-последовательности к старшим [12].

Таким образом, в настоящее время остается актуальной проблема совершенствования стохастических методов защиты данных.

Цель работы - получение алгоритма шифрования, преобразующего исходное сообщение в шифркод, который не обладает вероятностными связями, то есть представляет собой совокупность независимых значений, что существенно усложняет раскрытие зашифрованного текста.

МАТЕМАТИЧЕСКАЯ ПОСТАНОВКА ЗАДАЧИ

Предположим, что для некоторого словаря $\overline{X_l} = \{x(1),...,x(l)\}$ (соответствие между символами и их числовыми значениями может быть выбрано, например, $x_i = i$) стохастические связи букв $X(i) = x_j,\ j = \overline{1,l}$ в словах характеризуются матрицей $M[X^{\nu}(i)X^{\mu}(j)], i, j = \overline{1,I}, \nu, \mu = \overline{1,N-1}, \nu + \mu \le N$ (взаимосвязь букв в различных словах является слабой и ею можно пренебречь). Необходимо получить алгоритм шифрования, преобразующий каждое слово $X(i), i = \overline{1,I}$ (I - количество букв в слове) исходного сообщения в шифркод стохастически независимых значений $V_i, i = \overline{1,I}$.

РЕШЕНИЕ

Сначала получим линейный алгоритм шифрования.

Соответствие между первой буквой $X(1)$ последовательности $X(i), i = \overline{1,I}$ и значением V_1 шифркода может быть выбрано произвольным образом, например, $V_1 = X(1)$.

Второе значение представим в виде:

$$V_2 = X(2) - V_1\varphi_1(2), \tag{1}$$

$\varphi_1(2)$ - неслучайная координатная функция, удовлетворяющая условию $M[V_1V_2] = 0$, что дает:

$$\varphi_1(2) = \frac{M[V_1X(2)]}{M[V_1^2]} = \frac{M[X(1)X(2)]}{M[X^2(1)]}. \tag{2}$$

Третье значение V_3 шифркода определяется из соотношения:

$$V_3 = X(3) - V_1\varphi_1(3) - V_2\varphi_2(3), \tag{3}$$

где: $\varphi_1(3), \varphi_2(3)$ также вычисляются из условия $M[V_1V_3] = 0, M[V_2V_3] = 0$.

Очевидно, что:

$$\varphi_1(3) = \frac{M[V_1X(3)]}{M[V_1^2]} = \frac{M[X(1)X(3)]}{M[X^2(1)]}, \tag{4}$$

$$\varphi_2(3) = \frac{M[V_2X(3)]}{M[V_2^2]}, \tag{5}$$

учитывая выражение (1), получаем:

$$\varphi_2(3) = \frac{M[X(2)X(3)] - M[X^2(1)]\varphi_1(2)\varphi_1(3)}{M[X^2(2)] - M[X^2(1)]\varphi_1^2(2)}. \tag{6}$$

Для V_4 справедливо:

$$V_4 = X(4) - V_1\varphi_1(4) - V_2\varphi_2(4) - V_3\varphi_3(4). \tag{7}$$

Координатные функции: $\varphi_1(3), \varphi_2(3), \varphi_3(4)$ обеспечивают выполнение условий $M[V_1V_4]=0, M[V_2V_4]=0, M[V_2V_4]=0$:

$$\varphi_1(4)=\frac{M[V_1X(4)]}{M[V_1^2]}=\frac{M[X(1)X(4)]}{M[X^2(1)]}, \tag{8}$$

$$\varphi_2(4)=\frac{M[V_2X(4)]}{M[V_2^2]}=\frac{M[X(2)X(4)]-M[X^2(1)]\varphi_1(2)\varphi_1(4)}{M[X^2(2)]-M[X^2(1)]\varphi_1^2(2)}, \tag{9}$$

$$\varphi_3(4)=\frac{M[V_3X(4)]}{M[V_3^2]}. \tag{10}$$

С использованием (3) соотношение для определения $\varphi_3(4)$ в окончательном виде:

$$\varphi_3(4)=\frac{M[X(3)X(4)]-M[X^2(1)]\varphi_1(3)\varphi_1(4)M[X(3)X(4)]-M[X^2(1)]\varphi_1(3)\varphi_1(4)}{M[X^2(3)]-M[X^2(1)]\varphi_1^2(3)-M[X^2(2)]\varphi_2^2(3)}. \tag{11}$$

Каким образом, для одинаковых нижних индексов координатные функции имеют одинаковую форму записи (выражения (2),(4),(8) и (6),(10)) .

Обобщая рассуждения на произвольное число букв $X(i), i=\overline{1,I}$, получаем следующие соотношения для V_i [14]:

$$V_i=X(i)-\sum_{\nu=1}^{i-1}V_\nu\varphi_\nu(i), i=\overline{1,I}, \tag{12}$$

$$\varphi_\nu(i)=\frac{M[V_\nu X(i)]}{M[V_\nu^2]}=\frac{M[X(\nu)X(i)]-\sum_{j=1}^{\nu-1}M[V_j^2]\varphi_j(\nu)\varphi_j(i)}{M[V_\nu^2]}, \tag{13}$$

$$M[V_\nu^2]=M[X^2(\nu)]-\sum_{j=1}^{\nu-1}M[V_j^2]\varphi_j^2(\nu)\cdot \tag{14}$$

С помощью выражений (12)-(14) слово $X(i)=x(i), i=\overline{1,I}$ преобразуется в шифр-последовательность некоррелированных случайных коэффициентов $V_i, i=\overline{1,I}$.

Для маскировки в шифртексте вероятностных связей более высоких порядков построим соответствующий алгоритм преобразования начального сообщения.

Соответствие между первым значением шифркода и символом открытого текста оставим без изменения:

$$W_1^{(1)} = X(1). \tag{15}$$

Значение шифркода $W_2^{(1)}$ для второй буквы не должно учитывать стохастические связи $M[X^{\nu}(1)X(2)], \nu = \overline{1, N-1}$. В этой связи необходимо сформировать дополнительные значения $W_1^{(\nu)}, \nu = \overline{1, N-1}$, такие что $M[W_1^{(\nu)} W_1^{(\mu)}] = 0, \nu, \mu = \overline{1, N-1}, \nu + \mu \le N$, каждое из которых содержит информацию о $X^{\nu}(1), \nu = \overline{N-1}$. Требование $M[W_1^{(\nu)} W_1^{(\mu)}] = 0$, во-первых, существенно упрощает процедуру получения последующих значений шифркода $W_2^{(1)} ... W_I^{(1)}$ и, во-вторых, распространение данного ограничения на все $W_i^{(\nu)}, i = \overline{1, I}, \nu, = \overline{1, N-1}$, каждое из которых определяет $X^{\nu}(i), i = \overline{1, I}, \nu, = \overline{1, N-1}$, обеспечивает выполнение главного условия постановки задачи – отсутствие в шифркоде стохастических связей произвольного порядка. Значение $W_1^{(2)}$ представим в виде:

$$W_1^{(2)} = X^2(1) - W_1^{(1)} \beta_{21}^{(1)}(1). \tag{16}$$

С учетом требования ортогональности $W_1^{(1)}, W_1^{(2)}$ значение координатной функции $\beta_{21}^{(1)}(1)$ определяется из выражения:

$$\beta_{21}^{(1)}(1) = \frac{M[W_1^{(1)} X^2(1)]}{M[\{W_1^{(1)}\}^2]} = \frac{M[X^3(1)]}{M[X^2(1)]}. \tag{17}$$

Для $W_1^{(3)}$ имеют место соотношения:

$$W_1^{(3)} = X^3(1) - W_1^{(1)} \beta_{31}^{(1)}(1) - W_1^{(2)} \beta_{31}^{(2)}(1), \tag{18}$$

$$\beta_{31}^{(1)}(1) = \frac{M[W_1^{(1)} X^3(1)]}{M[\{W_1^{(1)}\}^2]}, \tag{19}$$

$$\beta_{31}^{(2)}(1) = \frac{M[W_1^{(2)} X^3(1)]}{M[\{W_1^{(2)}\}^2]}. \tag{20}$$

Используя выражения (15),(16) для $W_1^{(1)}, W_1^{(2)}$, формулы (19),(20) приводятся к окончательному виду:

$$\beta_{31}^{(1)}(1) = \frac{M[X^4(1)]}{M[X^2(1)]}, \tag{21}$$

$$\beta_{31}^{(2)}(1)=\frac{M[X^5(1)]-M[X^4(1)]\beta_{21}^{(1)}(1)}{M[X(1)^4]-M[X(1)^2]\{\beta_{21}^{(1)}(1)\}^2}. \quad (22)$$

Обобщая рассуждения для произвольного $W_1^{(\nu)}, \nu=\overline{1,N-1,}$ получаем выражения:

$$W_1^{(\nu)}=X^{\nu}(1)-\sum_{j=1}^{\nu-1}W_1^{(j)}\beta_{\nu 1}^{(j)}(1), \nu=\overline{1,N-1,} \quad (23)$$

$$\beta_{\nu 1}^{(j)}(1)=\frac{M[W_1^{(j)}X^{\nu}(1)]}{M[\{W_1^{(j)}\}^2]}=\frac{1}{D_j(1)}(M[X^j(1)X^{\nu}(1)]-$$

$$-\sum_{l=1}^{j-1}D_l(1)\beta_{j1}^{(l)}(1)\beta_{\nu 1}^{(l)}(1)), \nu=\overline{1,N-1,} \quad (24)$$

$$D_j(1)=M[\{W_1^{(j)}\}^2]=M[X^{2j}(1)]-\sum_{l=1}^{j-1}D_l(1)\{\beta_{j1}^{(l)}(1)\}^2, j=\overline{1,N-1.} \quad (25)$$

Таким образом, дополнительные значения $W_1^{(\nu)}, \nu=\overline{1,N-1}$ определены и второе значение шифркода $W_2^{(1)}$ запишется как:

$$W_2^{(1)}=X(2)-\sum_{j=1}^{N-1}W_1^{(j)}\beta_{11}^{(j)}(2). \quad (26)$$

С учетом требования $M[W_1^{(j)},W_2^{(1)}]\neq 0, j=\overline{1,N-1}$ соотношение для вычисления $\beta_{11}^{(j)}(2), j=\overline{1,N-1}$ имеет вид:

$$\beta_{11}^{(j)}(2)=\frac{1}{D_j(1)}(M[X^j(1)X(2)]-\sum_{l=1}^{j-1}D_l(1)\beta_{j1}^{(l)}(1)\beta_{11}^{(l)}(2)), j=\overline{1,N-1.} \quad (27)$$

Обобщение полученных закономерностей дает возможность записать выражения для определения произвольного значения $W_i^{(\nu)}, \nu=\overline{1,N-1,}i=\overline{1,I,}$

$$W_i^{(\nu)}=X^{\nu}(i)-\sum_{k=1}^{i-1}\sum_{l=1}^{N-1}W_k^{(l)}\beta_{\nu k}^{(l)}(i)-\sum_{l=1}^{\nu-1}W_{\nu}^{(l)}\beta_{\nu i}^{(l)}(i), \nu=\overline{1,N-1,}i=\overline{1,I}, \quad (28)$$

$$D_j(i)=M[\{W_i^{(j)}\}^2]=M[X^{2j}(i)]-\sum_{k=1}^{i-1}\sum_{l=1}^{N-1}D_l(k)\{\beta_{jk}^{(l)}(i)\}^2-$$

$$-\sum_{l=1}^{j-1} D_l(i)\{\beta_{ji}^{(l)}(i)\}^2,\ j=\overline{1,N-1}, i=\overline{1,I} \tag{29}$$

$$\beta_{\nu k}^{(j)}(i)=\frac{M[W_k^{(j)}X^{\nu}(i)]}{M[\{W_k^{(j)}\}^2]}=\frac{1}{D_j(k)}(M[X^j(k)X^{\nu}(i)]-$$

$$-\sum_{p=1}^{k-1}\sum_{l=1}^{N-1} D_l(p)\beta_{jp}^{(l)}(k)\beta_{\nu p}^{(l)}(i)-\sum_{l=1}^{j-1} D_l(k)\beta_{jk}^{(l)}(k)\beta_{\nu k}^{(l)}(i), \nu=\overline{1,N-1}, i=\overline{1,I}. \tag{30}$$

Координатные функции $\beta_{\nu k}^{(l)}(i)$ описывают стохастические связи порядка $l+\nu, l, \nu=\overline{1,N-1}, l+\nu\le N$ между буквами i и $j, i,\ j=\overline{1,I}$. Массив коэффициентов $W_i^{(\nu)}, \nu=\overline{1,N-1}, i=\overline{1,I}$:

$$W=\begin{vmatrix} W_1^{(1)} & W_2^{(1)} & \dots & W_{I-1}^{(1)} & W_I^{(1)} \\ W_1^{(2)} & W_2^{(2)} & \dots & W_{I-1}^{(2)} & W_I^{(2)} \\ \dots & \dots & \dots & \dots & \dots \\ W_1^{(N-2)} & W_2^{(N-2)} & \dots & W_{I-1}^{(N-2)} & W_I^{(N-2)} \\ W_1^{(N-1)} & W_2^{(N-1)} & \dots & W_{I-1}^{(N-1)} & W_I^{(N-1)} \end{vmatrix}, \tag{31}$$

содержит информацию о массиве значений:

$$X=\begin{vmatrix} X(1) & X(2) & \dots & X(I-1) & X(I) \\ X^2(1) & X^2(2) & \dots & X^2(I-1) & X^2(I) \\ \dots & \dots & \dots & \dots & \dots \\ X^{N-2}(1) & X^{N-2}(2) & \dots & X^{N-2}(I-1) & X^{N-2}(I) \\ X^{N-1}(1) & X^{N-1}(2) & \dots & X^{N-1}(I-1) & X^{N-1}(I) \end{vmatrix}. \tag{32}$$

Следует отметить, что после выполнения процедуры шифрования нет необходимости передавать весь массив значений $W_i^{(\nu)}, \nu=\overline{1,N-1}, i=\overline{1,I}$, достаточно использовать в шифркоде только первую строку $W_i^{(1)}, i=\overline{1,I}$ массива W - все остальные значения могут быть определены с помощью выражений (28)-(30). Таким образом, предложенный подход к шифрованию данных не увеличивает в сравнении с алгоритмом (12)-(14) объем зашифрованного сообщения.

Алгоритмы (12)-(14) и (28)-(30) апробированы на украинском толковом словаре (22 тыс. слов). Значения некоторых параметров представлены в таблицах 1-6.

Table 1. Значения $M[X(i), X(j)], i, j = \overline{1,10}$ для украинского толкового словаря.

	1	2	3	4	5	6	7	8	9	10
1	211,3	156	168,2	172,9	175	174,8	173,3	171,4	172,9	178,8
2	156	208,7	149,3	162,2	162,5	161,9	159,6	158,6	158,2	164,5
3	168,2	149,3	217,3	173,5	174,1	174,7	173,3	170,9	173,5	178,8
4	172,9	162,2	173,5	244,5	182,4	180,6	180,9	178,7	180,5	187,2
5	175	162,5	174,1	182,4	246,2	184,9	179,4	181	182,2	191,2
6	174,8	169,9	174,7	180,6	184,9	249,8	184,7	174,8	184,6	187,8
7	173,3	159,6	173,3	180,9	179,4	184,7	249,5	181,6	173,2	192,9
8	171,4	158,6	170,9	178,7	181	174,8	181,6	246,6	183,6	175,5
9	172,9	158,2	173,5	180,5	182,2	184,6	173,2	183,6	252,8	191,5
10	178,8	164,5	178,8	187,2	191,2	187,8	192,9	175,5	191,5	269,4

Table 2. Значения $\varphi_\nu(i), \nu, i = \overline{1,10}$ для украинского толкового словаря.

	1	2	3	4	5	6	7	8	9	10
1	1	0,74	0,79	0,82	0,83	0,83	0,82	0,81	0,82	0,85
2	0	1	0,27	0,37	0,36	0,35	0,34	0,34	0,33	0,35
3	0	0	1	0,35	0,34	0,35	0,35	0,34	0,36	0,36
4	0	0	0	1	0,22	0,20	0,23	0,22	0,23	0,24
5	0	0	0	0	1	0,21	0,15	0,19	0,19	0,23
6	0	0	0	0	0	1	0,19	0,08	0,19	0,15
7	0	0	0	0	0	0	1	0,18	0,03	0,21
8	0	0	0	0	0	0	0	1	0,19	-0,02
9	0	0	0	0	0	0	0	0	1	0,18
10	0	0	0	0	0	0	0	0	0	1

Table 3. Значения $M[X^n(1), X(i)], i = \overline{1,10}, n = \overline{1,3}$ для украинского толкового словаря.

n \	1	2	3	4	5	6	7	8	9	10
1	211,3	156	168,2	172,9	175	174,8	173,3	171,4	172,9	178,8
2	3840	2695	2827	3138	3172	3204	3209	3179	3251	3440
3	75924	54026	54781	64635	64892	66918	67245	67187	71118	77619

Table 4. Значения $M[X^n(2), X(i)], i = \overline{1,10}, n = \overline{1,3}$ для украинского толкового словаря.

n \	2	3	4	5	6	7	8	9	10
1	208	149	162	162	161	159	158	158	164
2	4279	2504	2934	2968	2969	2962	2945	2974	3168
3	27445	49515	59630	61229	61978	62594	62482	64965	71864

Table 5. Значения $\beta_{11}^{(n)}(i), i = \overline{1,10}, n = \overline{1,3}$ для украинского толкового словаря.

n \	1	2	3	4	5	6	7	8	9	10
1	1	0,738	0,796	0,818	0,828	0,827	0,820	0,811	0,818	0,846
2	0	-0,040	-0,047	-0,052	-0,052	-0,055	-0,056	-0,055	-0,058	-0,062
3	0	0,001	0,001	0,002	0,001	0,001	0,001	0,001	0,001	0,001

Table 6. Значения $\beta_{12}^{(n)}(i), i=\overline{2,10}, n=\overline{1,3}$ для украинского толкового словаря.

n / i	2	3	4	5	6	7	8	9	10
1	1	0,110	0,208	0,194	0,181	0,165	0,172	0,146	0,155
2	0	-0,019	-0,013	-0,016	-0,019	-0,019	-0,019	-0,018	-0,020
3	0	0,003	0,002	0,002	0,002	0,003	0,003	0,003	0,002

Как видно из таблиц 5,6 значения $\beta_{11}^{(n)}(i), i=\overline{1,10}$ и $\beta_{12}^{(n)}(i), i=\overline{2,10}$ являются относительно малыми величинами, однако это не означает что данные параметры не влияют на формирование шифркода так как $\beta_{11}^{(n)}(i), i=\overline{1,10}$ и $\beta_{12}^{(n)}(i), i=\overline{2,10}$ умножаются в процессе шифрования на значения $W_1^{(3)}$ и $W_2^{(3)}$ третьего порядка.

Таблицы 1-6 получены при однократном использовании слова и не отражают частоту появления слова в определенном тексте. Для практического использования полученных алгоритмов шифрования необходимо, естественно, накапливать базу знаний вероятностных параметров по множеству текстов определенной тематики.

ВЫВОДЫ

Анализ стохастических методов шифрования данных показал, что существующие алгоритмы не позволяют полностью скрыть вероятностные связи исходного сообщения и, таким образом, совершенствование данных методов является на сегодняшний день актуальной проблемой.

Алгоритм шифрования (28)-(30) позволяет преобразовать каждое слово $\{X\}=X(i), i=\overline{1,I}$ открытого исходного сообщения в последовательность независимых значений и, таким образом, скрыть стохастические связи $M[X^{\nu}(i)X^{\mu}(j)], i, j=\overline{1,I}, \nu,\mu=\overline{1,N-1}, \nu+\mu\le N$ произвольного порядка N.

Выражение (28) является одной из разновидностей канонического разложения [15-19] исследуемой случайной последовательности $\{X\}$. Правомерность использованного похода подтверждается положением [17] о возможности построения канонического разложения последовательности $\{f_1(\bar{z}_1),\ldots,f_n(\bar{z}_n)\}$, где $\bar{z}_\nu, \nu=\overline{1,n}$ - векторная случайная величина, а $f_\nu(\ ), \nu=\overline{1,n}$ - нелинейная функция.

Алгоритм (28)-(30), также как и каноническое разложение, положенное в его основу, не накладывает существенных ограничений на класс исследуемых случайных последовательностей (линейность, марковость, стационарность, монотонность и т.д.)

Для маскировки множественных вероятностных связей может быть использовано соответствующее каноническое разложение [20].

ЛИТЕРАТУРА

Герасименко В.А.: Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоиздат, 1994.

Жельников В.: Криптография от папируса до компьютера. – М.:ABF, 1996.

Карякин Ю.Д.: Технология «AXIS-2000» защиты материальных объектов от подделки. Управление защитой информации. Минск, 1997.

Шеннон К.Э.: Теория связи в секретных системах. В кн.: Шеннон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963.

Диффи У., Хеллман М.Э.: Защищенность и имитостойкость: Введение в криптографию. ТИИЭР. 1979.

Молдавян А.А., Молдавян Н.А., Советов Б.Я.: Криптография. Санкт-Петербург, «Лань», 2000.

Гундарь К.Ю. Гундарь А.Ю. Янишевский Д.А.: Защита информации в компьютерных системах. – К.: "Корнейчук", 2000. –152 с.,

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

Иванов М.А.: Криптографические методы защиты информации в компьютерных системах и сетях. .-М.:КУДИЦ-ОБРАЗ,2001.-361с.

Alfred Menezes., Minghua Qu., Scott Vanstone. IEEE P1363, Part 4: Elliptic Curve Systems.1995.

Gong G., Lam C.C.Y. Linear Recursive Sequences over Elliptic Curves. 2001.http:citeseer.ist.psu.edu/449444.html.

Кулаков И.А.: Стохастические системы и их применение в криптографии. Дихотомические последовательности и генераторы. – Материалы 8-ой конференции «РусКрипто'2006».

Введение в криптографию / Под общ. ред. В.В. Ященко. М.: МЦНМО, 2000.

Линейный стохастический алгоритм шифрования, базирующийся на каноническом разложении случайной последовательности. //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, Випуск 2(15) 2007 р. с.63-67.

Левин Б.Р.: Теоретические основы статистической радиотехники. т. 2.-М.:Сов. радио, 1968.- 503 с.

Васильев Б. В.: Прогнозирование надежности и эффективности радиоэлектронных устройств. - М.: Сов. радио, 1970.- 335 с.

Пугачев В.С. Теория случайных функций и ее применение.-М.:Физматгиз, 1962.-720с.

Кудрицкий В.Д.: Фильтрация, экстраполяция и распознавание реализаций случайных функций. – К.:ФАДА, ЛТД, 2001.-176 с.

Кудрицкий В.Д.: Прогнозирование надежности радиоэлектронных устройств.-К.:Техніка, 1982.- 168 с.

Атаманюк И.П.: Алгоритм реализации нелинейной случайной последовательности на базе ее канонического разложения. // Электронное моделирование.- 2001.-№5.с.38-46.

CRYPTOGRAPHIC PRIV ON BASE OF VEHICLE OF CANONICAL DECOMPOSITIONS OF CASUAL SEQUENCES

Summary. The article deals with the encoding method that makes it possible to transform a sent message into a sequence of uncorrelated values. The method makes the basic data extrapolation essentially harder. The algorithm is based on canonical decompression of examined casual sequence.

Key words: algorithm of encoding, linear stochastic connections.

Reviewer: Director of institute of automation and electrical engineers of the National university of shipbuilding named admiral Makarov, doctor of engineering sciences, professor Vladimir Blinchov.