Eastern-European Journal of Enterprise Technologies

jet.com.ua

ВОСТОЧНО-ЕВРОПЕЙСКИЙ ЖУРНАЛ ПЕРЕДОВЫХ ТЕХНОЛОГИЙ

ISSN 1729-3774

3/3 (33)
2008

информационные технологии
інформаційні технології
information technologies

новая экономика
нова економіка
new economy

промышленные технологии
промислові технології
industrial applications

ми на загальноєвропейському ринку міжнародних перевезень.

Література

1. Альошинський Є. С., Мкртичьян Д. І., Шелехань Г. І. Пропозиції по удосконаленню технології контейнерних перевезень України // Збірник наукових праць. — Харків: УкрДАЗТ, 2007. — Вип. 80. — с. 70–75.
2. Технологічний процес роботи залізничної станції Одеса-Порт Одеської залізниці. — Одеса. — 1999.
3. Технологічний процес роботи залізничної станції Іллічівськ Одеської залізниці. — Іллічівськ. — 2002.
4. Альошинський Є. С., Ломотько Д. В. Розробка моделі функціонування пунктів переробки контейнерних вантажів з використанням мереж Петрі // Восточно-европейский журнал передовых технологий. № 1/2 (31). — Харьков. — 2008.
5. Альошинський Є. С., Кіхтєва Ю. В. Принципи логістичного дослідження роботи прикордонних передавальних станцій// Восточно-европейский журнал передовых технологий. № 1/2 (25). — Харьков. — 2007. — с. 96–99.

УДК 681.3.06

ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ ШИФРОВАНИЯ ДАННЫХ НА БАЗЕ АППАРАТА КАНОНИЧЕСКИХ РАЗЛОЖЕНИЙ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

И. П. Атаманюк
кандидат технических наук
доцент кафедры высшей и прикладной математики
Николаевский государственный аграрный университет
54010, Украина, г. Николаев, ул. Парижской Коммуны, 9
Контактный тел.: (0512) 218301. **E-mail:** atamanyuk_igor@mail.ru

В роботі отримано алгоритм шифрування, який дає змогу перетворити повідомлення, що передається, в послідовність попарно незалежних значень. Алгоритм базується на канонічному розкладі випадкової послідовності, що досліджується

1. Постановка задачи

Одной из разновидностью криптографических систем, как известно [1–6], являются стохастические алгоритмы шифрования. Однако, принадлежащие к данному классу методы (дихотомические операторы, алгоритмы шифрования на эллиптических кривых) не позволяют получить из исходного сообщения шифркод абсолютно случайных независимых значений. В [7] предложен алгоритм шифрования, который позволяет преобразовать слова $\{x(1), ..., x(I)\}$ исходного сообщения в последовательность некоррелированных значений $\{v_1, ..., v_I\}$ ($x(i)$, $i=\overline{1, I}$ — числовое значение i-буквы, $M[X(i)X(j)]\neq 0$, $i, j=\overline{1, I}$, v_i, $i=\overline{1, I}$ — значение шифр-кода, $M[V_iV_j]=0$, $i, j=\overline{1, I}$):

$$V_i = X(i) - \sum_{v=1}^{i-1} V_v \varphi_v(i), \quad i=\overline{1, I}, \tag{1}$$

$$\varphi_v(i) = \frac{M[V_v X(i)]}{M[V_v^2]} = \frac{M[X(v)X(i)] - \sum_{j=1}^{v-1} M[V_j^2]\varphi_j(v)\varphi_j(i)}{M[V_v^2]}, \tag{2}$$

$$M[V_v^2] = M[X^2(v)] - \sum_{j=1}^{v-1} M[V_j^2]\varphi_j^2(v). \tag{3}$$

Алгоритм (1)–(3) базируется на каноническом разложении [8] случайной последовательности $\{X\}=X(i)$, $i=\overline{1, I}$, реализациями которой являются слова некоторого языка.

Однако, недостатком данного алгоритма является скрытие в шифр-коде только корреляционных связей и, таким образом, является актуальной задача получения метода преобразования исходного сообщения в шифркод, который не обладает стохастическими связями более высокого порядка.

Пусть вероятностные свойства последовательности $\{X\}=X(i)$, $i=\overline{1, I}$, описывающие особенности появления слов в некотором языке, заданы дискретизированной функцией $M[X^v(i)X^\mu(j)]$, $i, j=\overline{1, I}$, $v, \mu=\overline{1, N-1}$, $v+\mu\leq N$, т. е. предполагаются известными стохастические связи порядка N.

Необходимо получить алгоритм преобразования значений исходного сообщения $\{X\}=X(i)$, $i=\overline{1, I}$ в последовательность независимых значений шифр-кода $\{W\}=W_i^{(1)}$, $i=\overline{1, I}$.

2. Решение

Первому значению шифр-кода поставим в соответствие, например, первое значение исходного сообщения:

$$W_1^{(1)} = X(1). \quad (4)$$

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

$$W_1^{(2)} = X^2(1) - W_1^{(1)}\beta_{21}^{(1)}(1). \quad (5)$$

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

$$\beta_{21}^{(1)}(1) = \frac{M[W_1^{(1)}X^2(1)]}{M[\{W_1^{(1)}\}^2]} = \frac{M[X^3(1)]}{M[X^2(1)]}. \quad (6)$$

Для $W_1^{(3)}$ имеет место соотношение

$$W_1^{(3)} = X^3(1) - W_1^{(1)}\beta_{31}^{(1)}(1) - W_1^{(2)}\beta_{31}^{(2)}(1), \quad (7)$$

$$\beta_{31}^{(1)}(1) = \frac{M[W_1^{(1)}X^3(1)]}{M[\{W_1^{(1)}\}^2]}, \quad (8)$$

$$\beta_{31}^{(2)}(1) = \frac{M[W_1^{(2)}X^3(1)]}{M[\{W_1^{(2)}\}^2]}. \quad (9)$$

Используя выражения (4), (5) для $W_1^{(1)}$, $W_1^{(2)}$, формулы (8), (9) приводятся к окончательному виду

$$\beta_{31}^{(1)}(1) = \frac{M[X^4(1)]}{M[X^2(1)]}, \quad (10)$$

$$\beta_{31}^{(2)}(1) = \frac{M[X^5(1)] - M[X^4(1)]\beta_{21}^{(1)}(1)}{M[X(1)^4] - M[X(1)^2]\{\beta_{21}^{(1)}(1)\}^2}. \quad (11)$$

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

$$W_1^{(v)} = X^v(1) - \sum_{j=1}^{v-1} W_1^{(j)}\beta_{v1}^{(j)}(1), \quad v=\overline{1, N-1}, \quad (12)$$

$$\beta_{v1}^{(j)}(1) = \frac{M[W_1^{(j)}X^v(1)]}{M[\{W_1^{(j)}\}^2]} = \frac{1}{D_j(1)}(M[X^j(1)X^v(1)] -$$

$$-\sum_{l=1}^{j-1} D_l(1)\beta_{jl}^{(1)}(1)\beta_{vl}^{(l)}(1)), \quad v=\overline{1, N-1}, \quad (13)$$

$$D_j(1) = M[\{W_1^{(j)}\}^2] =$$

$$= M[X^{2j}(1)] - \sum_{l=1}^{j-1} D_l(1)\{\beta_{jl}^{(l)}(1)\}^2, \quad j=\overline{1, N-1}. \quad (14)$$

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

$$W_2^{(1)} = X(2) - \sum_{j=1}^{N-1} W_1^{(j)}\beta_{11}^{(j)}(2). \quad (15)$$

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

$$\beta_{11}^{(j)}(2) = \frac{1}{D_j(1)}(M[X^j(1)X(2)] -$$

$$-\sum_{l=1}^{j-1} D_l(1)\beta_{jl}^{(l)}(1)\beta_{1l}^{(l)}(2)), \quad j=\overline{1, N-1}. \quad (16)$$

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

$$W_i^{(v)} = X^v(i) - \sum_{k=1}^{i-1}\sum_{l=1}^{N-1} W_k^{(l)}\beta_{vk}^{(l)}(i) - \sum_{l=1}^{v-1} W_v^{(l)}\beta_{vi}^{(l)}(i),$$

$$v=\overline{1, N-1}, \ i=\overline{1, I}, \quad (17)$$

$$D_j(i) = M[\{W_i^{(j)}\}^2] = M[X^{2j}(i)] -$$

$$-\sum_{k=1}^{i-1}\sum_{l=1}^{N-1} D_l(k)\{\beta_{jk}^{(l)}(i)\}^2 - \sum_{l=1}^{j-1} D_l(i)\{\beta_{ji}^{(l)}(i)\}^2,$$

$$j=\overline{1, N-1}, \ i=\overline{1, I}, \quad (18)$$

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

$$-\sum_{p=1}^{k-1}\sum_{l=1}^{N-1} D_l(p)\beta_{jp}^{(l)}(k)\beta_{vp}^{(l)}(i) - \sum_{l=1}^{j-1} D_l(k)\beta_{jk}^{(l)}(k)\beta_{vk}^{(l)}(i),$$

$$v=\overline{1, N-1}, \ i=\overline{1, I}. \quad (19)$$

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

$$W = \begin{vmatrix} W_1^{(1)} & W_2^{(1)} & \dots & W_{I-1}^{(1)} & W_I^{(1)} \\ W_1^{(2)} & W_2^{(2)} & \dots & W_{I-1}^{(2)} & W_I^{(2)} \\ \dots & \dots & \dots & \dots & \dots \\ W_1^{(N-2)} & W_2^{(N-2)} & \dots & W_{I-1}^{(N-2)} & W_I^{(N-2)} \\ W_1^{(N-1)} & W_2^{(N-1)} & \dots & W_{I-1}^{(N-1)} & W_I^{(N-1)} \end{vmatrix} \quad (20)$$

содержит информацию о массиве значений

$$X = \begin{vmatrix} X(1) & X(2) & \dots & X(I-1) & X(I) \\ X^2(1) & X^2(2) & \dots & X^2(I-1) & X^2(I) \\ \dots & \dots & \dots & \dots & \dots \\ X^{N-2}(1) & X^{N-2}(2) & \dots & X^{N-2}(I-1) & X^{N-2}(I) \\ X^{N-1}(1) & X^{N-1}(2) & \dots & X^{N-1}(I-1) & X^{N-1}(I) \end{vmatrix} \quad (21)$$

Следует отметить, что после выполнения процедуры шифрования нет необходимости передавать весь массив значений $W_i^{(v)}$, $v=\overline{1, N-1}$, $i=\overline{1, I}$, достаточно использовать в шифр-коде только первую строку $W_i^{(1)}$, $i=\overline{1, I}$ массива W — все остальные значения могут быть определены с помощью выражений (17)–(19). Таким образом, предложенный подход к шифрованию данных не увеличивает по сравнению с алгоритмом (1)–(3) объем зашифрованного сообщения.

Алгоритм апробирован на украинском толковом словаре (22 тыс слов). Значения некоторых параметров представлены в **табл. 1–4**.

Таблица 1

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

n \ i	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

Таблица 2

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

n \ i	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

Таблица 3

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

n \ i	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

Таблица 4

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 **табл. 3, 4** 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 шифр-кода 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.

Табл. 1–4 получены при однократном использовании слова и не отражают частоту появления слова в определенном тексте. Для практического использования алгоритма шифрования (17)–(19) необходимо, естественно, накапливать базу знаний вероятностных параметров по множеству текстов определенной тематики.

3. Выводы

Алгоритм шифрования (17)–(19) позволяет преобразовать каждое слово $\{X\}=X(i)$, $i=\overline{1, I}$ открытого исходного сообщения в последовательность независимых значений и, таким образом, скрыть стохастические связи $M[X^v(i)X^\mu(j)]$, $i, j=\overline{1, I}$, $v, \mu=\overline{1, N-1}$, $v+\mu \le N$ произвольного порядка N.

Выражение (17) является одной из разновидностей канонического разложения исследуемой случайной последовательности {X}. Правомерность использованного похода подтверждается положением [4] о возможности построения канонического разложения последовательности $\{f_1(\overline{z}_1), ..., f_n(\overline{z}_n)\}$, где $\overline{z}_v$, $v=\overline{1, n}$ — векторная случайная величина, а $f_v(\ )$, $v=\overline{1, n}$ — нелинейная функция.

Алгоритм не увеличивает объем шифр-кода по сравнению с (1)–(3) и 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.).

Литература

1. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. — М.: КУДИЦ-ОБРАЗ, 2003. — 240 с.
2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: КУДИЦ-ОБРАЗ, 2001. — 361 с.
3. Alfred Menezes., Minghua Qu., Scott Vanstone. IEEE P1363, Part 4: Elliptic Curve Systems, 1995.